ASD-TR-84-5010

AD-A145 651

AVIONICS INTEGRITY PROGRAM (AVIP) - VOLUME I
Procurement Phase Issues - Design,
Manufacturing, and Integration

BATTELLE MEMORIAL INSTITUTE
COLUMBUS LABORATORIES
COLUMBUS, OHIO 43201

Donald Eldredge

Ellis F. Hitt

Richard K. Thatcher

Larry D. Scurlock

MARCH 1984

TECHNICAL REPORT ASD-TR-84-5010
Final Report for Period September 1983 to March 1984

DTIC FILE COPY

Approved for Public Release;
Distribution is Unlimited.

DTIC

AERONAUTICAL SYSTEMS DIVISION
AVIONICS INTEGRITY PROGRAM OFFICE
DIRECTORATE OF AVIONICS ENGINEERING
AIR FORCE SYSTEMS COMMAND
WRIGHT-PATTERSON AIR FORCE BASE, OHIO

84 09 05 121

NOTICE

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely related Government procurement operation, the United States Government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

This report has been reviewed by the Office of Public Affairs (ASD/PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

LEE F. CHESHIRE, Major, USAF
Program Manager
Avionics Integrity Program
Directorate of Avionics Engineering

THOMAS J. DICKMAN
Technical Director
Avionics Integrity Program
Directorate of Avionics Engineering

FOR THE COMMANDER

GARY L. LUDWIG
Technical Director
Directorate of Avionics Engineering
Aeronautical Systems Division
Wright-Patterson Air Force Base, Ohio

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	Approved for public release; distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
	ASD-TR-84-5010

6a. NAME OF PERFORMING ORGANIZATION	6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
Battelle Memorial Institute	Section 685	Avionics Integrity Program Office

6c. ADDRESS (City, State and ZIP Code)	7b. ADDRESS (City, State and ZIP Code)
Battelle Columbus Laboratories 505 King Avenue Columbus, Ohio 43201	Aeronautical Systems Division Wright-Patterson AFB, Ohio 45433

8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
	ASD/ENAS/AVIP	F33657-83-C-0229

8c. ADDRESS (City, State and ZIP Code)	10. SOURCE OF FUNDING NOS.			
	PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.
Wright-Patterson Air Force Base, Ohio 45433	64	2734	0000 632531	

11. TITLE (Include Security Classification)
See Reverse

12. PERSONAL AUTHOR(S)
Eldredge, Donald; Hitt, Ellis F.; Thatcher, Richard K.; Scurlock, Larry D.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Final	FROM Sept 83 TO Mar 84	March 1984	226

16. SUPPLEMENTARY NOTATION
One of four reports delivered under contract stated in Block 9. See Report FOREWORD for further information.

17.	COSATI CODES		18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	
13	08		See Reverse
14	02		

19. ABSTRACT (Continue on reverse if necessary and identify by block number)
This report addresses program phases of design, manufacturing and integration. It includes assessments of methodologies of work which can be used to develop a proven, tolerant product capable of withstanding the use environment. The goal of the process described is to eliminate defective piece parts, processes and final product, prior to delivery to the purchasing activity. A tolerable systems engineering process, dealing with activities that are known to take place during each phase can be developed through use of the material provided.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS ☐	UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE NUMBER (Include Area Code)	22c. OFFICE SYMBOL
John Kaufhold	(513)-255-3369	ASD/ENAS/AVIP

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE

BLOCK 11.   TITLE: AVIONICS INTEGRITY PROGRAM (AVIP) STUDIES: Procurement Phase Issues - Design, Manufacturing, and Integration

BLOCK 18.   SUBJECT TERMS: Pre-Request for Proposal (FP) requirements, defined environment, physical use environment, stress screening, environmental assessment, thermal cycling, reliability growth, failure diagnosis, avionics integration abd documentation, integrity criteria, defects, build-to-print, processes control, parts derating, burn in, computer aided design (CAD), design software-hardware integration.

VOLUME I: DESIGN, INTEGRATION, AND MANUFACTURING PHASE ISSUES

TABLE OF CONTENTS

TABLE OF CONTENTS
(Continued)

TABLE OF CONTENTS
(Continued)

c

LIST OF TABLES

LIST OF TABLES
(Continued)

e

LIST OF FIGURES

This report is one of a series of four prepared for the Avionics Integrity Program Office, Wright-Patterson Air Force Base, Ohio. The reports address techniques and historical data (lessons learned) for enhancing the service life of avionic systems. The reports include contractor efforts between September 1983 and March 1984.

Each report represents a completed study in a specific area and stands alone. However, the contents of the four reports are meant to complement each other and they should be considered as the output of a single study aimed at determining those issues which contribute to the avionics integrity of military systems.

The titles of the remaining reports and their respective technical report numbers are provided as follows:

> ASD-TR-84-5009, AVIONICS INTEGRITY PROGRAM (AVIP) STUDIES: Program Cost Assessment - Environmental Stress Screening and Diagnostic Techniques, Volume III

> ASD-TR-84-5011, AVIONICS INTEGRITY PROGRAM (AVIP) STUDIES: Hardware Case Studies, Volume II

> ASD-TR-84-5012, AVIONICS INTEGRITY PROGRAM (AVIP) STUDIES: Force Management - Economic Life Considerations, Volume IV

These reports have been entered into the DTIC/NTIS system. Contact the Avionics Integrity Program focal point ((513)255-3369) to obtain the appropriate report number for ordering.

The authors wish to acknowledge the cooperation and consideration afforded to them by Mr. Thomas Dickman, Mr. John Kaufhold, and Major Lee Cheshire of the Avionics Integrity Program Office during the conduct of these studies. Without their continuing guidance and interest, these reports could not have been developed. The authors would also like to thank Mr. Tom Dolash, Mr. Keith Broerman, Susan Hendershot, Nanci Peterson, and the Text Processing Center personnel at Battelle Columbus Laboratories for their contribution to these reports.

i

GLOSSARY

ACCELERATED TEST - A test conducted on an equipment at a higher level of environmental severity than would be experienced in operational service, including the application of operating cycles at an accelerated rate. The primary purpose of an accelerated test is to reduce the time required to prove an equipment's capability and to establish its limits of operation. Analysis of data from an accelerated test is usually empirical. Where practical, accelerated tests should be conducted using combined environments, especially those considered critical.

ACTIVE REPAIR TIME - That portion of downtime during which one or more technicians are working on that system to effect a repair.

ASSEMBLY - A number of parts or subassemblies joined together to perform a specific function.

ASSURANCE - The relative confidence or certainty that specific program objectives will be achieved.

AVAILABILITY - The probability that an item will be operationally ready to perform its function where called upon at any point in time. Steady state availability of installed equipment is a function of equipment mean-time-between-failures (MTBF) and equipment mean downtime (MDT), as follows:

$$A = \frac{MTBF}{MTBF + MDT}$$

AVAILABILITY, ACHIEVED - The probability that a system is operating satisfactorily at any point in time when used under stated conditions, where the time considered includes operating and active repair time along with preventive maintenance downtime.

AVAILABILITY, INHERENT - The availability potential of a given design configuration under ideal support conditions (i.e., no logistics waiting time). Inherent availability, which includes only corrective maintenance time, mean-time-to-repair, is given by:

$$A_1 = \frac{MTBF}{MTBF + MTTR}$$

AVAILABILITY, INTRINSIC - The probability that the system is operating satisfactorily at any point in time when used under stated conditions, where the time considered is operating time and active repair time.

AVAILABILITY, OPERATIONAL - The probability that a system is operating satisfactorily at any point in time when used under stated conditions, where the time considered includes operating, active repair time, preventive maintenance downtime, and an additional term which is the additional time accumulated by those circumstances that combine to delay the active repair process.

iii

BURN-IN - The operation of an item to induce infant mortality failures before field use in order to stabilize its operational characteristics upon commissioning to those expected for the useful life period.

CORRECTIVE MAINTENANCE - Actions performed, as a result of failure, to restore an item to a specified level of performance.

CORRECTIVE MAINTENANCE ACTION - Action required to repair a single failure; comprising all those individual maintenance tasks involved in the maintenance procedure (e.g., fault localization, isolation, repair, checkout, etc.).

DELAY TIME - The component of downtime during which no maintenance is being accomplished on the item because of technician alert and response time, supply delay, or administrative reasons.

DEMONSTRATED RELIABILITY - The level of reliability that is proven, by analysis of test or in-service data, to be achieved.

DEMONSTRATION - Proof of the achievement of a quantitative goal or requirement. It may involve formal demonstration testing or may be based on data from development tests and in-service usage.

DERATING - The intentional reduction of stress/strength ratio in the application of an item, usually for the purpose of reducing the occurrence of stress-related failures.

DESIGN REVIEW - A meeting of capable representatives from organizational units which affect or are affected by the design documents. The purpose of the design review meeting is to openly review all aspects of the design concepts and related documentation in an effort to insure the incorporation of sound engineering principles, including reliability, maintainability, producibility, etc., in the final design for the product.

Design reviews are the responsibility of the Design Office and are usually held early in the preliminary design phase, at the start of detailed design, and prior to design freeze. Design decisions are made by the Chief Design Engineer based on inputs and questions from the various representatives.

Multipurpose design verification procedure and project management tool used to evaluate the reliability and maintainability, life cycle cost, performance, and various other characteristics of an equipment at major design and testing milestones.

DISCRIMINATION RATIO (DR) - The ratio of specified MTBF (θ_0) to the minimum acceptable MTBF (θ_1) expressed as

$$DR = \theta_0/\theta_1$$

DOWNTIME - The period of time during which an item is not in a condition to perform its intended function.

DURABILITY - The ability of an avionic system to exist and to meet established performance criteria and system stresses in the operational environment for a long time without significant deterioration or non-economical maintenance characteristics.

ELEMENT - One of the constituent parts of anything. An element, in fact, may be a part, a subassembly, an assembly, a unit, a set, etc.

ENVIRONMENT - The aggregate of all the external conditions and influences affecting the life and development of the product.

EQUIPMENT - One or more units and necessary assemblies, subassemblies, and parts, connected or associated together and including all necessary interconnecting cabling, hydraulic lines, accessories, etc., to perform an operational function (e.g., radio receiving set, missile, radar set). An equipment is not normally a replaceable item.

ENVIRONMENTAL TEST - A test to discover the effects upon system performance, reliability, and safety of the several environments to which the system would be exposed during its life cycle. Often it is only necessary to test the system under the separate environments which affect the system most critically but combinations of environments must be evaluated as well. The final environmental test, of course, is under actual use conditions, in the target vehicle.

EXPECTED VALUE - Normally, the average value of a random variable. The expected value is also the unbiased estimate of the variable but not necessarily the "best" statistical estimate. When dealing with the estimate of the standard deviation of a Normal distribution, we usually use the formula for the "expected" or unbiased estimate rather than the sample standard deviation, especially where the sample is small. If the experiment from which we have made our estimate of the variable were repeated many times and estimates made each time, we could expect the average of all those estimates to be the expected value. This principle is also applicable to estimating reliability.

FAILURE - An equipment will be considered to have failed when it no longer operates within the required performance limits of the specification and requires unscheduled maintenance, unscheduled adjustment, or replacement of parts to restore its performance within limits. Precise definitions of failure for each part, component, subsystem, and system should be made prior to any test program.

FAILURE ANALYSIS - An investigation of a failure which has already occurred. The purpose of a failure analysis is to determine the primary cause of failure so that corrective action can be taken to preclude recurrence of that failure. Failure analyses often require the services of specialists such as metallurgists, chemists, stress analysts, and electronic engineers to pinpoint the primary cause of failure.

FAILURE LAW, EXPONENTIAL - The exponential failure law states that the probability of survival, P_S, of an equipment operating for a time, T, is a function of the mean life, m, or of a failure rate, λ, as expressed by the following:

$$P_S = e^{-T/m} \qquad\qquad P_S = e^{-\lambda T}$$

FAILURE MECHANISM - A basic physical process or change which is responsible for the observed failure mode; the process of degradation or the chain of events which results in a particular failure mode.

FAILURE MODE - A particular way in which a part can fail. A shaft in the Auxiliary Power Unit can fail in torsion, shear, and bending, and by centrifugal force; a resistor failure can be a short or an open condition.

FAILURE MODE AND EFFECT ANALYSIS - An analysis of a particular design for describing, as a minimum, the most probable ways an equipment can fail and the consequences of these failures. The FMEA can include probability of occurrence for each failure mode, the visible symptoms of occurrence, the design corrective actions which can be taken, remedial actions which should be taken, etc. The primary purpose of the FMEA activity is to reveal ways an equipment can fail so that corrective action can be taken in the design phase, which is by far the least costly time in the program. FMEA's are also used to provide data for use in trouble shooting and isolation.

FAILURE RATE (λ) - The frequency of occurrence of failures in a group of systems or parts, usually measured in terms of failures per unit of operating time. If there are 12 steering control valves in service which have accumulated 67,000 hours and have experienced five failures, the failure rate is 5/67,000 or 0.000075 failures per valve operating hour. Failure rates can be expressed in terms of percent and/or per multiples of hours (e.g., for the steering control valve, the failure rate is expressible as 7.5% per thousand hours).

FAULT DETECTION TIME - Time between the occurrence of a failure and the point at which it is recognized that the system or equipment does not respond to operational demand.

FAULT LOCALIZATION - A man/machine task to determine which particular major unit of equipment is at fault, by making use of malfunction symptoms, test equipment, and features built into the equipment.

INHERENT RELIABILITY - The characteristic of an equipment which describes its design potential for reliability, considering the state of the art of processes, procedures, and materials. Inherent reliablity is the direct result of design effort which involves the design engineer in the use of

vi

simplicity, proven practices, design development, and, in certain instances, redundancy. Inherent reliability tends to degrade in the subsequent cycles of fabrication, assembly, shipping, handling, checkout testing, etc., so that the in-service reliability of an equipment is never more than its inherent reliability.

INTEGRITY (AVIONICS) - The characteristic of an avionic system to perform its intended function (specified performance and system availability) under operational conditions for a specified service life at a minimum life cycle cost.

LEVEL OF SEVERITY - The degree of stress resulting from a particular degree of external environment upon an equipment. Also known as "stress level". To illustrate, excessive air loads on a wing panel cause structural members to yield under combined stresses. Maximum voltage across a transistor can cause it to perform with little or no margin and therefore a low level of reliability. Greater than normal or expected levels of environment are sometimes imposed upon a product in test in order to establish its margin of operation to provide a measure of reliability.

LIFE CYCLE COST - The total cost of acquisition, operation, maintenance, and support of an item throughout its useful life.

LIFE, USEFUL - The total operating time in which an item remains operationally effective and economically useful before wearout.

MAINTAINABILITY - A measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure, expressed as the probability that an item will be retained in or restored to a specified condition within a given period of time when the maintenance is performed in accordance with prescribed procedures and resources.

MAINTAINABILITY DEMONSTRATION TESTS - Acceptance tests (performed by the contractor) usually at the equipment or subsystem level for the major items which will comprise the integrated system to demonstrate conformance to specified quantitative maintainability requirements.

MAINTAINABILITY ENGINEERING - The engineering discipline which formulates an acceptable combination of design features, repair policies, and maintenance resources, to achieve a specified level of maintainability, as an operational requirement, at optimum life cycle costs.

MAINTENANCE - The act of diagnosing and physically repairing/restoring, or preventing, equipment failures.

MAINTENANCE ANALYSIS - The process of identifying required maintenance functions by analysis of the design, to determine the most effective means to accomplish these functions.

MAINTENANCE CAPABILITIES - The facilities, tools, test equipment, drawings, technical publications, trained maintenance personnel, engineering support, and spare parts required to restore a system to serviceable conditions.

MAINTENANCE CONCEPT - A description of the planned general scheme for maintenance support of an item in the operational environment. The maintenance concept provides the practical basis for design, layout, and packaging of the system and its test equipment and establishes the scope of maintenance responsibility for each level of maintenance and the personnel resources (maintenance manning and skill levels) required to maintain the system.

MAINTENANCE DOWNTIME RATE - Equipment downtime per operating hour, comprising downtime due to corrective maintenance and downtime required for preventive maintenance.

MAINTENANCE TASK - Actions required to preclude the occurrence of a malfunction or restore an equipment to satisfactory operating condition.

MALFUNCTION - The performance of a functional part beyond specified limits. If the malfunction of a part requires unscheduled maintenance, adjustment or replacement, it is usually considered a failure.

MAXIMUM TIME TO REPAIR - The maximum time required to complete a specified percentage of all maintenance actions.

MEAN CORRECTIVE MAINTENANCE TIME - The mean time required to complete a maintenance action, i.e., total maintenance downtime divided by total maintenance actions, over a given period of time. Mean time to repair (often denoted as MTTR) is the sum of all maintenance downtime during a given period divided by the number of maintenance actions during the same period of time.

MEAN-CYCLES-BETWEEN-FAILURES - The average number of cycles between failures, said of an equipment but calculated from a group of such equipments. The MCBF is found by dividing the number of failures encountered, over a given time interval, into the total number of operating cycles experienced by all such equipments during that time interval. MCBF is similar to mean-time-between-failures (MTBF) except is applicable to cyclic equipment rather than time-sensitive equipment. Relays, switches, on-off valves, and actuators are examples of cyclic hardware.

MEAN DOWNTIME - The average time an equipment is down during a maintenance action and during which the system is not in condition to perform its intended function. Downtime is subdivided into the following categories: active repair time and supply delay time.

MEAN PREVENTIVE MAINTENANCE TIME - The mean (or average) equipment downtime required to perform scheduled preventive maintenance on the item, excluding any preventive maintenance time expended on the equipment during operation and excluding administrative and supply delay downtime.

MEAN TIME BETWEEN FAILURES - The average number of hours between failures, said of an equipment but calculated from a group of like equipments by dividing the total operating time on all the equipments during a given time period by the number of failures experienced in the group during the given time period.

MEAN TIME BETWEEN FAILURES - MTBF (θ) is equal to the total operating time of the equipment divided by the number of failures. (The MTBF is also the reciprocal of the failure rate.)

MEAN TIME BETWEEN FAILURES, MINIMUM ACCEPTABLE (θ_1) - A value so selected that an associated and specific risk of accepting equipment of the value is tolerable.

MEAN TIME BETWEEN FAILURES, SPECIFIED (θ_0) - The MTBF value specified in the contract of equipment specification. Its value is determined by multiplying the minimum acceptable MTBF by the discrimination ratio of the selected test plan. It is used to limit producers risk (α).

$$\theta_0 = (\theta_1) \cdot (\theta_0/\theta_1)$$

MEAN TIME TO REPAIR - The mean time required to complete a maintenance action, i.e., total active maintenance downtime (i.e., fault isolation, fault correction, calibration, and checkout) divided by the total number of maintenance actions, over a given period of time, excluding those time elements which are related to preparation and delay, administrative, and supply delay, downtime.

MEAN TIME TO RESTORE - That time associated with reinitiation of the system's functional capabilities. For nonredundant systems, this time is usually equivalent to MTTR. In the case of standby redundant systems, or systems where a different hardware type cn provide back-up service, system restoration time is equal to the time required to switch operation to the back-up unit. It is computed by dividing the total system outage time by the number of system outages over a given period of time.

MEAN TIME BETWEEN UNSCHEDULED REMOVALS - The average number of hours between unscheduled removals of a component or system. Unscheduled maintenance is a direct function of reliability in that the longer the time between failures, the less unscheduled maintenance is required. The MTBUR for a component is calculated as follows:

$$\text{MTBUR} = \frac{\text{total aircraft hours x components per aircraft}}{\text{number of unscheduled removals}}$$

MEDIAN CORRECTIVE MAINTENANCE TIME - The downtime within 50% of all corrective maintenance actions can be completed under the specified maintenance conditions. The median value, M_{ct}, is often referred to as the geometric mean (MTTR_G) or equipment repair time (ERT) in some maintainability documents.

MEDIAN PREVENTIVE MAINTENANCE TIME - The equipment downtime required to perform 50% of all scheduled preventive maintenance actions on the equipment under the specified conditions.

MISSION RELIABILITY - That reliability of an item which is associated with the functional purpose of the item; the probability of an item performing its intended function. If a heat exchanger fan for the air conditioning system is supposed to run continuously for 2.2 hours for each 1.8 hour flight, its mission is 2.2 hours; if its reliability is 0.997, then we could expect three failures in a thousand flights or 2,200 operating hours. Reliabilities may also be associated with separate portions of a total mission, for example, cruise reliability, climb reliability, or taxi, lineup and take-off reliability.

PART - An element of a subassembly, or an assembly, of such contruction that it is not practical to dissassemble the element for maintenance purposes.

PREVENTIVE MAINTENANCE - A procedure in which the system is periodically checked and/or reconditioned in order to prevent or reduce the probability of failure or deterioration in subsequent service.

PROBABILITY (P [ ]) - The likelihood of a certain event occurring. A probability can be zero (cannot occur) or one (certain to occur) or any value in between, usually expressed as a decimal but can be shown as a percentage.

PROBABILITY DISTRIBUTION - A graphical representation (bar chart, histogram or curve) of the relative probability of a random variable taking on values between certain limits. A probability distribution is similar to a frequency distribution except that the sum of the discrete probabilities and the total area under the continuous curve which represents probability are equal to 1.0. In a discrete distribution, the variable can take only certain fixed, predetermined values, whereas in a continuous distribution, the variable can assume any of an infinite number of values between two limits. Bar charts and histograms are used to represent discrete probability distributions. Examples of a continuous probability distribution are the familiar bell-shaped Normal distribution and the Exponential distribution.

PRODUCT RULE - If a group of components are comprised in a system and all of them must operate properly for the system to function successfully, then the reliability of the system, expressed as a probability, is numerically equal to the product of the reliabilities of the separate components. A quick approximation can usually be made by adding the failure probabilities or unreliabilities (1.0 minus reliability) of the compnents and subtracting the sum from 1.0.

In a parallel arrangement of components (redundancy), it is the "unreliability" of the system which is equal to the product of the individual component unreliabilities. That product is then subtracted from 1.0 to obtain the system reliability.

QUALITY ASSURANCE (QA) - The effort exerted to assure product compliance with applicable drawings and specifications. Responsibility for the quality assurance effort belongs to groups performing hardware inspections, procurement, reliability assurance functions, process control, and production testing.

RANDOM FAILURE - A failure which is <u>unpredictable in time</u>. Random failures can be predicted only in terms of the probability of their occurrence in time. Failures can occur in a system test in an unpredictable manner; that is, we cannot predict just when a specific failure will occur, but we can still predict the probability of experiencing that failure during a given time period, providing of course that it has not already occurred prior to that period. Random failures are dealt with by the designer in the same manner as the "predictable" ones--design action to preclude their occurrence or recurrence is one of his primary objectives. Randomness is particularly applicable for describing the failure pattern of a complex system where the cause-effect pattern for each failure mode cannot be practically known but probability predictions can be made relative to the entire group of failure modes.

REDUNDANCY - The existence of more methods to perform a particular function than are actually required to perform the function. Redundancy incorporates parts in parallel, either as actively redundant or as standby redundant.

REDUNDANCY, ACTIVE - That redundancy wherein all redundant items are operating simultaneously rather than being switched on when needed.

REDUNDANCY, STANDBY - That redundancy wherein the alternative means of performing the function is inoperative until needed and is switched on upon failure of the primary means of performing the function.

RELIABILITY - The commonly accepted definition of reliability is that it is the mathematical probability of an equipment performing as intended.

A reliability of 0.94 or 94% for an equipment means theoretically that there is a probability of 0.94 that a randomly selected equipment will perform properly when commanded to do so. However, a more practical definition is that, of a group of these equipments selected randomly, 0.94 or 94% of them will perform properly and 6% will fail.

Reliability is also defined as the probability that an item will perform the intended function for a specified time interval under stated operational and mission requirements/conditions.

RELIABILITY, INHERENT - The reliablity potential in a mature design configuration when all design discrepancies are corrected.

RELIABILITY, PREDICTED - The reliability of an equipment computed from its design considerations and from the reliability of its parts in the intended conditions of use.

RELIABILITY DEMONSTRATION TESTS - Acceptance tests (performed by the contractor) usually at the equipment or subsystem level for the major items which will comprise the integrated system to demonstrate conformance to specified quantitative reliability requirements.

RELIABILITY ENGINEERING - The engineering discipline which formulates an acceptable combination of design features, repair philosophy, and maintenance resources, to achieve a specified level of reliability as an operational requirement, at optimum life cycle costs.

RELIABILITY GOAL - That level of reliability which is desired for the product. A reliability goal is a target to shoot for but not usually contractually binding upon the producer; reliability which is binding with penalties and/or rewards for the producer are referred to as a reliability requirement and represents a minimum acceptable to the customer.

RELIABILITY GROWTH - The gradual increase in actually achieved reliability of an equipment as the result of changes made due to knowledge gained from test or operational experience. Reliability growth comes about when weaknesses of a design, a procedure, or a material are discovered and corrective action is taken to preclude the effect of the weakness on the equipment. If a failure mode can be eliminated or its probability of occurrence drastically reduced for a particular item, the reliability of that item is directly increased by this amount of decrease in probability of failure. Reliability growth can be exponential in the early phases of a program.

RELIABILITY PREDICTION - The forecast or estimate made in the design phase of what reliabilities or failure rates can be associated with the existing designs, considering the state of the art of design concepts, processes, and materials. Reliability predictions involve generic failure data on similar parts, past data on specific parts, and engineering judgment. Consideration is given also to performance requirements, operational environments, and their interrelationships. Reliability predictions are used to show where reliability program emphasis is needed for greatest effectiveness.

RELIABILITY PROGRAM - A concentrated effort by the company's organizational units working together to accomplish certain reliability objectives. Primary responsibility falls to the program and project managements, the project design engineers, and Reliability Engineering.

The quality assurance groups have the primary responsibility in the hardware production part of the program. There are many other groups involved directly or indirectly in the reliability program, the elements of which are described in the reliability program plan written for the particular project. These other groups include the functions of procurement, test, field representatives, the customer, subcontractors, suppliers, and the many supporting functions too numerous to list here. The scope of a reliability program is such as to include the effort required for designing reliability into the product, retaining reliability during

xii

the processes performed on the hardware, improving reliability of substandard hardware, and providing proof of reliability achievement.

RELIABILITY REQUIREMENT - Refers to a level of reliability which is a minimum acceptable to the customer, as opposed to a reliability goal which is a target to shoot for. If demonstration of achievement of the reliability requirement is made contractual by the customer, with associated rewards and penalties, there will also be a minimum acceptable confidence level to which the proof of achievement must be demonstrated. Reliability requirements are appropriately apportioned to subcontractors and suppliers who support the particular program.

RELIABILITY TEST - Although the term would usually refer to a test as part of a formal reliability demonstration program, there are other types of reliability test on parts and components to determine margins of operation or potential failure modes. In fact, nearly all tests contribute some data or information toward making reliability estimates or judgments, especially if they expose the equipment to environment on life type test where real weaknesses can be discovered.

SCREENING - The process of performing 100% inspection on product lots (all products or a sample basis) and removing the defective units from the lots.

SCREENING TEST - A test or combination of tests, intended to remove unsatisfactory items or those likely to exhibit early failures.

SEQUENTIAL TESTING - A statistically based method of testing in which decision making for reliability proof of achievement is a continuous process in time rather than a periodic one. The decision to be made in a sequential test is to accept the test as having demonstrated achievement of the reliability requirement, to reject the test, or to continue testing because the trend shown by the data is too weak to make a safe decision. The method of sequential testing is the most efficient method in time of testing for proof of reliability achievement but it does involve the predetermination of the subtle constants α and β, the risks we are willing to take in making incorrect decisions to accept or reject the demonstration.

SERVICING - The performance of any act (other than preventive or corrective maintenance) required to keep an item of equipment in operating condition, such as lubricating, fueling, oiling, cleaning, etc., but does not include periodic replacement of parts or any corrective maintenance tasks.

SINGLE FAILURE POINT - A single item of hardware, the failure of which would lead directly to the total loss of the hardware system performance.

SPECIFICATION - A document intended primarily for use in procurement which describes the essential technical requirements for items, including the procedures by which it will be determined that the requirements will be

met. A detailed description of the characteristics of a product and of the criteria which must be used to determine whether the product is in conformity with the description.

STRESS - The physical force, load or external condition imposed upon an item tending to degrade its performance, reliability or safety margin. A failure is the result of the stress upon an item exceeding its strength. For an item of given strength, increasing stress decreases reliability.

STRESS ANALYSIS - The evaluation of stress conditions (electrical, thermal, vibration, shock, humidity, etc.) under which parts are applied in the design of a system or equipment. On the basis of a stress analysis, failure rates are appropriately adjusted to reflect the deleterious effects of the stresses on the reliability of the parts involved.

SUBASSEMBLY - Two or more parts which form a portion of an assembly, or form a unit replaceable as a whole, but having a part or parts which are replaceable as individuals.

SUBSYSTEM - A major subdivision of a system that performs a specified function in the overall operation of a system.

SUCCESS - A success occurs when an equipment operates without failure, within performance tolerances, in the operating environment, and for the required length of time or for the required number of cycles when commanded to do so. Also, success is one of the parameters used in estimating reliability when utilizing attributes data.

SUCCESS RATIO - The ratio of the number of successes observed during an experiment, test or service aplication to the total number of observations made up of successes and failures. The success ratio is frequently used as a point estimate of an achieved reliability or probability of success.

In dealing with the binomial distribution, the success ratio is referred to statistically as the "maximum likelihood estimate" of reliability. Success ratios of zero or 1.0 may require additional interpretation before being of practical value.

SYSTEM - A combination of complete operating subsystems, equipments, assemblies, subassemblies, components, parts, or accessories interconnected to perform a specific operational function.

SYSTEM EFFECTIVENESS - The overall capability of a system to accomplish its mission, usually expressed as a probability and as such is the product of the probabilities related to reliability (how long), performance (how well), and availability (how often). An equipment which has a relia- bility of 0.995 and a performance capability of 0.990 but an availability of only 0.78 has an overall effectiveness as follows:

$$S = (0.990)(0.78)(0.995)$$
$$S = 0.768$$

The overall effectiveness is always less than the least of the three factors.

TIME, ADJUSTMENT OR CALIBRATION - That element of Maintenance Time during which the needed adjustments of calibrations are made.

TIME, CHECKOUT - That element of Maintenance Time during which performance of an item is verified to be in specified condition.

TIME, FAULT CORRECTION - That element of Maintenance Time during which a failure is corrected by (a) repairing in place; (b) removing, repairing, and replacing; or (c) removing and replacing with a like serviceable item.

TIME, PREPARATION - That element of Maintenance Time needed to obtain the necessary test equipment and maintenance manuals, and set up the necessary equipment to initiate fault location.

TRADE-OFF - The process by which a designer can evaluate one or more proposed design considerations in terms of possible effects in other areas and make an intelligent decision based upon these evaluations.

UNIT - An assembly or any combination of parts, subassemblies, and assemblies mounted together, and normally capable of independent operation in a variety of situations.

WEAROUT FAILURE - A failure which occurs as the result of deterioration processes or mechanical wear. The probability of occurrence of wearout failures normally increases with time and is often characterized by the Normal frequency distribution. Wearout failures generally occur near the end of the useful life of an item and are usually characterized by mechanical or chemical action.

WORST CASE ANALYSIS - A design analysis to determine the effects upon a system reliability if all its components function at their tolerance extremes. A worst case analysis considers the effects of dimensional limits as well as the limits of performance parameters. Normally, if at least the major equipments at functional extremes do not degrade system reliability below the acceptable minimum, the margin of operation can be considered adequate.

1.0 INTRODUCTION

In current and next generation aircraft, the implementation of advanced technologies, new design concepts, embedded computer systems and software based digital systems is changing the traditional role of avionics, flight controls, engine controls, weapon delivery systems and man-machine interfaces. Greater amounts of integration and commonality of functions are becoming a reality in existing systems, with flight critical functions and mission essential functions becoming more integrated and the integrity requirements becoming more complex and more important in order for the aircraft to be available to perform its intended mission. These systems, however, often do not live up to their analytically (or otherwise) derived reliability, availability and other integrity parameter predictors when they are deployed in their operational environment.

The effectiveness of our military force depends in part on the operational readiness of its weapon systems. In the case of the U.S. Air Force, a major item which affects the operational readiness of an aircraft is the condition of the avionics equipment, particularly safety-of-flight or mission essential equipment. To assure that operational readiness is achieved at reasonable operating and support costs, avionics equipment must be designed to meet that objective early in the context of a well defined system engineering process. Specific design requirements' evaluation criteria and integrity parameters and measures must be stated in the procuring agencies' statement of work; and plans must be formulated by the manufacturer or system integrator to meet those requirements. The environment in which the equipment must operate, be maintained or stored must be defined and redefined as the system requirements are specified and the development proceeds. The initial prototype hardware and software must be tested, analyzed, fixed and evaluated with respect to the actual aircraft environment. Software must be developed not only to perform operational functions but to allow accurate diagnostics to be performed through built-in test and fault isolation tests. In addition, software must also be integrated into the system using Hot Bench systems under control of a realistic and complete subsystem/system integration plan. Once the hardware design is proven, proper manufacturing discipline must be applied to ensure that quality parts and workmanship are combined in an efficient manufacturing process. The equipment must be built-to-print and properly tested, analyzed and fixed before being released to final test and inspections. Finally, the fielded equipment's use and handling must be closely and objectively scrutinized, especially for the initial delivered units. The results from the final environmental stress screening, acceptance tests and handling (package and storage) of the system must be compared against the environment planned and used for the design. Discrepancies between the designed system and the "as-built" system may seriously compromise the integrity of the system, and, when it is deployed, may require additional analyses and examination of both the environment and mission, and the delivered equipment (SRU and LRU's) to determine if the delivered product will meet the expected operational life and life cycle cost for the system.

1.1 BACKGROUND

The Avionics Integrity program was established specifically to
improve the avionics acquisition process by increasing awareness of the trade-
offs available during the system life cycle. The major emphasis for AVIP is
the current perception that complex avionics systems are often not living up
to their reliability and availability predictions when they reach the field.
The fact that these systems fail to meet analytically derived criteria (i.e.,
predicted MTBF) is often explained by the fact that, at the time, existing
budget and manpower constraints faced by avionics acquisition programs reduce
the amount of emphasis placed on the measures of avionics integrity during the
systems' life due to insufficient planning time and higher development costs.
Thus, tradeoffs may have been made in the early phases of a program which did
not take the parameters of integrity fully into account. Therefore, hardware
problems appear after the validation and full scale development phases which
impact program costs through required engineering changes and increased repair
time and spares provisioning. The program's aim of early emphasis on integ-
rity by the combined Air Force/Industry team, will be to identify integrity
parameters, and methods which provide the technical emphasis needed to iden-
tify and correct problems prior to when the systems are fielded.

"AVIP is an Aeronautical Systems Division, Deputy for Engineering
initiative to develop an orderly plan and procedure to assure that USAF
acquire reliable, high quality, supportable avionics with a higher avail-
ability than presently achieved. The effort, modelled after the successful
Aircraft Structural Integrity Program (ASIP) and the newer Engine Structural
Integrity Program (ENSIP), utilizes a multidisciplined systems engineering
approach to identify and eliminate causes of lowered system integrity. AVIP
is a guide to both Air Force and industry to identify a proper balance between
cost, performance and schedule where the trades may influence system integrity
throughout the life cycle. Integrity is a combination of such parameters as
reliability, maintainability, manufacturing quality, producibility, lifetime,
supportability, and availability. It is intended that AVIP will specify what
procedures are necessary to achieve that balance in the system acquisition
phase. The prime thrust is the definition of the key technical and management
activities which must be accomplished at particular times during the acquisi-
tion process to assure a balance of cost, schedule, performance and integrity
over the avionics system's projected life."[1,2]

In terms of scope, AVIP is targeted for avionics systems which
include flight critical functions (such as flight controls) as well as mission
essential functions. AVIP techniques are to be applied to any avionics hard-
ware design independent of whether the avionics is part of an advanced devel-
opment program, supplied as GFE to a Systems Integrator or procured from an
existing commercial vendor. Furthermore, it is intended that the AVIP tech-
niques will be applied to current as well as future ("new") procurements
and/or avionics upgraded in currently existing systems.

1.2 SCOPE

This report addresses three major subsystem/system acquisition phases: design, integration and manufacturing. The three phases are addressed in the framework of a systems engineering process dealing with the activities that are known to take place during each phase as well as alternatives which might be used for a given activity assuming that alternatives exist or are available. The activities of the various phases are presented, then evaluated and analyzed in terms of their effect on each of the defined integrity parameters -- as applicable.

1.3 REFERENCES

1. Draft Military Standard, Avionics Integrity Program (AVIP),
    MIL-STD-XXXX(11), ASD/ENAS, Wright-Patterson AFB, Ohio, 10 July, 1983.

2. The Avionics Integrity Program (AVIP), Dickman, T. J., and Cheshire, L. F.
    (Major), Federal Acquisition Research Conference/Symposium, December,
    1983.

2.0 ANALYSIS OF SYSTEM ACQUISITION PHASE
ACTIVITIES AND THEIR RELATIONSHIP TO
INTEGRITY PARAMETERS

2.1 DESIGN PHASE ACTIVITIES ANALYSIS

The Avionics Integrity Program has defined a process and implemented a process flow diagram consisting of five stages--the first three of which are related to the Design Phase. The first stage, the Design Information Stage encompasses development of the Avionics Integrity Master Plan, completion of a system and subsystem allocation of requirements, initiation of an Avionics Integrity Historical Document record, and concludes with the completion of a preliminary system design. The second stage, the Preliminary Design stage, develops the allocated system and Line Replaceable Unit details to allow a technically competitive source selection. During this stage, the preliminary trades, assessments and analyses are conducted. The third stage, the Design, Analysis and Development stage, includes conduct of trades and analyses, testing of prototypes to arrive at product specifications. The key activities identified in this stage include use of detailed stress analysis to establish derating criteria in the design; the trade analyses based on life cycle cost and integrity allocation; and test, analyze and fix feedback activity in conjunction with detailed failure diagnoses.

In order to properly analyze the design phase, it is necessary first to define four (4) distinct activity sub-phases and then to define the specific activities that occur during each sub-phase. Next, an analysis of the various activities/variables will be done in terms of the integrity parameters that these activities/variables affect. In addition, the analysis will be carried forward to the examination and specification of the analytically derived criteria which can be used to estimate the integrity parameters and the related measures which may be available to demonstrate the integrity of the system. The major product of these analyses will be a table relating the various activities to the integrity parameters, estimated criteria and measures. The four (4) design sub-phase activities which result in deliverables, are:

Activity	Section
● Procurement Agency Design Sub-Phase	2.1.1
● Contractor's Preliminary Design Sub-Phase (including Preliminary Design Review (PDR)).	2.1.2
● Contractor's Detailed Design Sub-Phase (including Critical Design Review (CDR)).	2.1.2
● Contractor's Prototype Development Sub-Phase (Including Test Analyze and fix).	2.1.3

The Procurement Agency Design Sub-Phase activities are presented in Section 2.1.1, the Contractor's Preliminary Design Sub-Phase and the Detailed Design Sub-Phase activities are combined and presented in Section 2.1.2; and

the Contractor's Prototype Development Sub-Phase activities are presented in Section 2.1.3.

2.1.1 Procurement Agency Design Sub-Phase

An important consideration during the procuring agencies' Design Phase, in analyzing the user's problem is that of selecting and specifying attributes of quality that are called for by the problem. Usability is a composite attribute that needs to be designed into the product. Usability is generally composed of those qualities known as reliability, testability, maintainability, efficiency, understandability and adaptability. The definition of the user's problem must include not only the required functions and their performance characteristics, but also the quality of the product that is required to fulfill the user's needs. Furthermore, in order to properly evaluate each of these activities in terms of integrity characteristics, it is necessary to be able to relate the identified activities/sub-activities and their inputs/outputs to the integrity characteristics. Table I-2.1-1 contains a list of the relevant tools, parameters, criteria, and measures which are the integrity characteristics that are available to demonstrate or determine that integrity has been designed into the product from its basic inception to delivery and use of the final product. This compiled list should then be applied to each of the relevant activities within the appropriate design phase.

The decisions made with respect to the above enables the user to state the problem, to determine the environment in which the user operates as well as resources available, and to identify the attributes of quality for the final product. Once the decisions are known and made, they can be formalized into a logical definition of requirements; which can be specified in terms of:

- A description of the physical environment in which the system is to operate.
- The other systems with which there will be an interface.
- The people who will work with the system.
- The functions that the system is to perform.
- The data required by the system or output by the system (format, frequency, accuracy, resolution, timing).

Once formalized, these requirements need to be documented according to the standards established by the procuring organization in the context of a formal design phase consisting of four (4) specific activities:

1.1 System Requirements Analysis

1.2 Detailed Specifications Preparation

1.3 Procurement Package Generation

1.4 Source Selection.

TABLE 1-2.1-1. LIST OF RELEVANT TOOLS, PARAMETERS, CRITERIA, AND MEASURES APPROPRIATE TO AVIONICS INTEGRITY

Tools	Parameters	Criteria	Measures
Statistical Distribution	Availability	MTBF (Mean Time Between Failures)	Failure & Time
Weibull Distribution Function	Lifetime (Durability)	MTTR (Mean Time to Repair)	Predicted
Exponential Distribution Function	Maintainability	MCT (Mean Down Time)	Measured
Normal Distribution Function	Repairability	MTBUR (Mean Time Between Unscheduled Removals)	Time (Calendar/Clock)
Statistical Computations	Supportability	MTBR (Mean Time Between Removals)	Predicted
Mean/Standard Deviation	Testability	MTBMA (Mean Time Between Maintenance Actions)	Measured
Correlation (Variances/Covariances)	Manufacturing Quality	MMT (Mean Maintenance Time)	Go/No Go Decisions
Regression (Linear/Non-Linear)	Manufacturing Technology Assessment		Criteria Determination
Deterministic	Producibility		Meets
Stochastic	Quality Assurance		Does Not Meet
Simulation/Models	Reliability		Costs Development
Cost Analysis Models			Logistics
Performance Analysis Models			Maintenance
Reliability Prediction/Assessment Models			Return-on-Investment
Fault Tree Analysis Models			Range
Failure Mode Effects and Criticality Analysis			Rating Scale(s)
Design Review			Judgment (Subjective)
Checklists			Adequate
Control Charts			Not Adequate
Nomographs			
Standardized Forms/Worksheets			
Plans			
Subjective Evaluation Criteria			
Computer Aided Design/Computer Aided Manufacture			
Test Equipment/Devices			

The material presented in Table I-2.1.1-1 relates the above activities/sub-activities of the Procurement Agencies Design Sub-Phase to the integrity characteristics presented in Table I-2.1-1. The material is presented in a matrix format with the design related activities on the left side and the integrity attributes on the right side.

From the data in Table I-2.1.1-1 it can be seen that most of the integrity measures are subjective responses as to whether or not the activity was performed. Even though these judgments are subjective, they still need to be made, and they need to be documented so that a record is available. In addition, standardized checklists need to be developed so that at each decision period the same criteria can be applied in making the evaluation. The input/output columns are important in that they contain a list of the products that are required in order to complete the various activities in a systematic manner.

2.1.2 Contractor's Preliminary and Detailed Design Sub-Phases

In the Preliminary and Detailed Design Sub-Phases, the product (sub-system/system) is transformed from a concept to reality by the input/output activities and functions that are performed by the design team. During the preliminary design sub-phase, the concept is established by the "paper" design which results from the initial assessment activities, the most important of these activities are shown in Table I-2.1.2-1 (Part 1).

The System Hardware Development Specification, the System Hardware Interface Specification, and the Completed Preliminary Hardware Design Description Report are all reviewed at a Hardware Preliminary Design Review. The results are documented in a formal report which is used in the Detailed Design Sub-Phase.

The activities performed in the Detailed Design Sub-Phase use the Preliminary Hardware Design Description Report and the results of the Hardware Preliminary Design Review as a basis for completing the design and establishing the final package to be forwarded for production. The events and activities which take place in this phase are also outlined in Table I-2.1.2-1 (Part 2).

Upon completion of the final Hardware Design Description Report, the Hardware Test reports, final specifications and drawings, and the final subsystem and components data report are submitted for the Critical Design Review. The activities leading up to the completion of the final hardware design are complex and varied, and as such, require many decisions and tradeoffs to be made which impact the reliability, maintainability, availability, and cost of the developing system. It is, therefore, important that the concept of integrity is not lost in the process of making decisions and tradeoffs. In order for the integrity issues to be incorporated in the final design, they must be planned for, and carried out, and their impact measured. Eight (8) design phases tools and activities have been identified which significantly impact the integrity of the final product, and these eight (8) will

TABLE 1-2.1.1.1. RELATIONSHIP OF PROCUREMENT AGENCIES DESIGN PHASE ACTIVITIES TO THE INTEGRITY ATTRIBUTES

Design Phase Activity/Actor	Sub-Activity	Input	Output	Tools	Integrity Parameter	Integrity Criteria	Integrity Measure
1. PROCUREMENT AGENCY							
1.1 System Requirements Analysis	Plan to Develop New System	--	System Analysis Report	--	--	--	--
	Program Management Plan	--	--	--	--	--	--
	Define Mission Performance Requirements/Operational Environment	System Analysis Report	System Requirements Report Environmental Assessment Report	ALPOS COSTER AEP AIROPS	Reliability Maintainability Repairability Supportability Availability Life Cycle Costs	MTBF MTTR MDT MTBUR (MTBF)	( ) Failure Rate (Based on Input Order a
	Define Reliability/Safety Criteria & Methods	--	Reliability/Safety Assessment	--	--	--	Was It Done?
	Define Subsystem/System Criticality Category	--	Function Criticality Report	--	--	--	Was It Done?
	Define Quantitative Mission Reliability Goals	Function Criticality Report System Requirements Report	Mission Reliability Goals Report	--	--	--	Was It Done?
	Finalize System Requirements	--	System Specification	--	--	--	Was It Done? Is It Complete?
1.2 Detailed Specifications Preparation	Select Applicable Standards	Existing: MIL-PRIME MIL-STD MIL-HDBK MIL-SPEC	List of Selected Standards for Procurement Package	--	--	--	--
	Perform Initial Reliability/ Maintainability Assessment	Environment Assessment Report Parts Failure Rates (Generic) System Specifications Supply Sources Parts List (Generic) Available Government Furnished Equipment	Initial Reliability/ Maintainability Assessment Parts Data Requirements List of GFE	Reliability Allocation Worksheets Generic: Parts Count Prediction Stress Analysis Prediction Maintainability Prediction Maintainability Analysis	Reliability Maintainability Life Cycle Costs	Correlation between MTBF and Subsystem/System Performance	Subjective Evaluation: Meets/Does Not Meet Target
	Perform Cost vs. Reliability/ Maintainability Trade Off Studies	--	--	--	Reliability Maintainability Life Cycle Costs	--	Return on Investment
	Define Candidate System Architectures	System Specification	Candidate System Architecture Report - Redundancy Requirements	--	Life Cycle Cost Availability	--	Logistics Costs Maintenance Support Costs
	Define Logistics Support Plan	--	--	--	Life Cycle Cost Maintainability Supportability Repairability	MDT MTTR	Was It Done? Logistics Costs Maintenance Support Costs Skill Levels/No. of Maint. Personnel
1.2 Detailed Specifications Preparation (continued)	Define Reliability and Maintainability Attributes & Application Levels	System Specifications Initial Reliability/ Maintainability Assessment Report List of Selected STD's Cand. System Architecture Report Function Criticality Report	Parts Selection Criteria Derating Modularity Diagnostics Reliability Growth Testing Stress Screening Tests Progress Monitoring Level Environmental Assessment Evaluation Criteria Report Physical Stress Level Analysis Criteria Report	--	All	All	Test Equipment Complexity Subjective Evaluation: Meets/Does Not Meet Criteria % Stress Level(s) for Environmental Stress Screening
1.3 Procurement Package Generated	Prepare Statement of Work	System Specification	--	--	All	Minimum Acceptable MTBF	--
	Establish Evaluation Criteria	Integrity Criteria	Source Selection Criteria	--	All	Target MTBF	Criteria Checklist
1.4 Source Selection	--	Knowledge of Company Facilities/Performance on Previous Contracts Source Selection Criteria Contractor Proposals (Including Management & Reliability/Maintainability Proposals) Manufacturing Process Approach (CAD/CAM) Environmental Assessment Evaluation	Contract Award	--	--	--	--

TABLE I-2.1.2-1. CONTRACTOR'S PRELIMINARY DESIGN PHASE AND DETAILED DESIGN PHASE ACTIVITIES

Part 1: Preliminary Design Phase Activities

Activity	Input	Output
1. Define Candidate System Architecture	System Specification, Function Criticality Report, Baseline Performance Requirements Report, Mission Reliability Goals Report, Environment Assessment Report	System Candidate Architecture Report
2. Develop Configuration Management Plan	Program Management Plan, System Specification	Configuration Management Plan
3. Obtain Candidate Subsystems and Components Data	System Candidate Architecture Report, Mission Reliability Goals Report, Physical Stress Level Analysis Report	Subsystems and Components Data Report, % Stress Level for Environmental Stress Evaluation/Tests
4. Perform Reliability Analysis	System Candidate Architecture Report, Subsystems and Components Data Report, Reliability/Safety Analysis Plan	Reliability Assessment Report
5. Perform Maintainability Analysis	System Candidate Architecture Report, Subsystems and Components Data Report, Reliability Assessment Report, Maintainability/Testability Plan	Maintainability Assessment Report
6. Establish Initial Man/Machine Task Allocation	Subsystem and Components Data Report, Fault Detection/Recovery Algorithms Report, Reliability Assessment Report, Maintainability Assessment Report	Workload Assessment Report
7. Partition/Allocate Functions to Hardware/Software	Candidate System Architecture Report, Workload Assessment Report, Subsystem and Component Data Report	Function Allocation Report
8. Review Reliability/Maintainability Assessment Analysis	Candidate System Architecture Report, Function Allocation Report, Subsystem and Components Data Reports, Reliability Assessment Report, Maintainability Assessment Report	Reliability/Maintainability Plan
9. Prepare System Hardware Design/Interface Specifications	System Specifications, System Candidate Architecture Report, Configuration Management Plan, Subsystems and Components Data Reports, Function Allocation Report, Reliability/Maintainability Plan, Environment Assessment Report, Physical Stress Level Analysis Report	System Hardware Development Specifications, System Hardware Interface Specifications, Completed Preliminary Hardware Design Description Report/Preliminary Drawings

Part 2: Detailed Design Phase Activities

Activity	Input	Output
1. Review Specifications	System Candidate Architecture Report, System Specification, Reliability/Maintainability Plan, System Hardware Development Spec, System Hardware Interface Spec, Preliminary Hardware Design Description Report	System Hardware Development Plan
2. Update Specifications and Drawings	Preliminary Drawings, Subsystem and Component Data Report, Reliability/Maintainability Plan, System Hardware Development Plan	Updated Specifications and Drawings, Updated Subsystem and Component Data Report (Parts Lists/Suppliers)
3. Board Design: Placement/Layout/Thermal Analysis/Power Dissipation	System Hardware Development Plan, Updated Specifications and Drawings, Subsystem and Component Data Report, Computer Aided Design Report, Environment Assessment Report, Physical Stress Level Analysis Report	Detailed Board Design and Analysis Report, Updated Specifications and Drawings, % Stress Level for Environmental Stress Evaluation/Tests
4. Breadboard/Evaluate Circuits	Detailed Board Design and Analysis Report, Hardware Test Plans, Updated Specifications and Drawings, Updated Subsystem and Components Data Report	Hardware Test Reports, Final Subsystem and Components Data Report, Final Specifications and Drawings
5. Prepare Final Hardware Design Description	Hardware Test Reports, Final Subsystem and Components Data Report, Final Specifications and Drawings	Hardware Design Description Report

be explored in detail in Appendix I-A-1 through I-A-8. The eight (8) tools and activities are:

      Appendix I-A-1 Section 2.1.2.1 Piece Parts Selection

      Appendix I-A-2 Section 2.1.2.2 Parts Derating

      Appendix I-A-3 Section 2.1.2.3 Parts Burn-in

      Appendix I-A-4 Section 2.1.2.4 Environmental Stress Screen

      Appendix I-A-5 Section 2.1.2.5 Failure Predictions

      Appendix I-A-6 Section 2.1.2.6 Computer Aided Design

      Appendix I-A-7 Section 2.1.2.7 Testability

      Appendix I-A-8 Section 2.1.2.8 Design Reviews.

The impact of each of these tools/activities and their importance to avionics integrity are discussed and analyzed, in terms of their input on the emerging design as well as their relationship to the integrity criteria, parameters, and measures.

In general, Table I-2.1.2-2 summarizes the effect of implementing the eight (8) design phase tools and activities during the preliminary and detailed design. From this table, it can be seen that:

(a) Each of the tools/activities impacts the integrity attributes of the developing product somewhat differently in that each tool/activity has its own unique set of integrity parameters, criteria, and measures.

(b) Each of the tools/activities affects its own unique set of preliminary and detailed design activities, with <u>piece part selection</u>, <u>parts derating</u>, <u>parts burn-in</u>, and <u>environmental stress screen</u> having the greatest impact on the emerging design in terms of the number of activities affected.

In addition to impacting the various preliminary and detailed design activities in terms of increased integrity, piece part selection, parts derating, parts burn-in, and environmental stress screening have the greatest impact on the cost of developing the emerging product. The selections and decisions made during these design phases can increase the overall cost due to more expensive parts being selected and/or more expensive or longer tests being specified in order to ensure that infant and latent defects due to parts, handling, or processes are detected, removed/replaced, and analyzed prior to fielding of the equipment.

TABLE I-12. THE EFFECTS OF IMPLEMENTING THE DESIGN PHASE TOOLS/ACTIVITIES ON THE INTEGRITY ELEMENTS

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.1. PIECE PART SELECTION	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (7) Partition/Allocate Functions to Hardware/Software (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/Interface Specifications	Reliability Maintainability Availability Repairability Supportability Life Cycle Cost	MTBF MTTR MDT MDR MMT	Failure Rate Logistics Costs (Spares Provision) Maintenance Support Costs Test Available Test Equipment Complexity
	DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description			
2.1.2.2. PARTS DERATING	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/Interface Specifications	Reliability Availability Life Cycle Cost Supportability Maintainability	MTBF MTBR MDT	Percent Electrical Stress Overload Acquisition Cost Design Constraints/Degree of Difficulty Maintenance Support Costs Operational Environment Reliability Growth
	DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description			
2.1.2.3. BURN-IN	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis	Reliability Life Cycle Cost Availability Maintainability	MTBF MTTF MTBR MDT MMT	Failure Rate (Early) Failure Rate (Late) Development Cost Logistics Costs (Spares Provision)
	DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description			
2.1.2.4. ENVIRONMENTAL STRESS SCREEN	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis	Reliability Life Cycle Cost Availability Maintainability	MTBF MTTF MTBR MDT MMT	Failure Rate (Early) Failure Rate (Late) Development Cost Logistics Costs (Spares Provision)
	DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design			

DETAILED DESIGN PHASE:
(2) Update Specifications and Drawings
(3) Board Design: Placement/Layout/ Thermal Analysis/Power Description
(4) Breadboard/Evaluate Circuits
(5) Prepare Final Hardware Design Description

2.1.2.5. FAILURE PREDICTION ANALYSIS

PRELIMINARY DESIGN PHASE:
(4) Perform Reliability Analysis
(5) Perform Maintainability Analysis
(8) Review Reliability/Maintainability Assessment Analysis
(9) Prepare System Hardware Design/ Interface Specifications

DETAILED DESIGN PHASE:
(2) Update Specifications and Drawings
(3) Board Design: Placement/Layout/ Thermal Analysis/Power Description
(4) Breadboard/Evaluate Circuits
(5) Prepare Final Hardware Design Description

Reliability
Availability
Maintainability
Life Cycle Cost

MTBF
MTTR
MTBR

Cost (Due to Redundancy Requirements)
Cost (Due to Component Selection)
Life Cycle Cost
Failure Rate
  • Fail Operational
  • Fail Safe
Manpower/Computer Costs to Perform Failure Prediction Analysis
Facility Costs (Hot Bench/Pallet for Fault Insertion/Data Collection)
Maintenance Support Costs

2.1.2.6. COMPUTER AIDED DESIGN

PRELIMINARY DESIGN PHASE:
(3) Obtain Candidate Subsystem and Components Data
(4) Perform Reliability Analysis
(5) Perform Maintainability Analysis
(8) Review Reliability/Maintainability Assessment Analysis
(9) Prepare System Hardware Design/ Interface Specifications

DETAILED DESIGN PHASE:
(1) Review Specifications
(2) Update Specifications and Drawings
(3) Board Design: Placement/Layout/ Thermal Analysis/Power Description
(4) Breadboard/Evaluate Circuits
(5) Prepare Final Hardware Design Description

Reliability
Maintainability
Availability
Repairability
Supportability
Produceability
Manufacturing Quality
Life Cycle Costs

MTBF
MTTR
MTBR
MDT
MMT

CAD/CAM Interface Costs
Life Cycle Costs
Development/Testing Costs
Data Base Costs
Production Costs
Time
Test Equipment Complexity

2.1.2.7. TESTABILITY

PRELIMINARY DESIGN PHASE:
(1) Define Candidate System Architecture
(5) Perform Maintainability Analysis
(6) Establish Initial Man/Machine Task Allocation
(7) Partition/Allocate Functions to Hardware/Software
(8) Review Reliability/Maintainability Assessment Analysis
(9) Prepare System Hardware Design/ Interface Specifications

DETAILED DESIGN PHASE:
(1) Review Specifications
(2) Update Specifications and Drawings
(4) Breadboard/Evaluate Circuits
(5) Prepare Final Hardware Design Description

Maintainability
Availability
Reliability
Testability
Life Cycle Cost

MTBF
MDT
MMT

Time (Diagnostic/Repair)
BIT/BITE/ATE
Trade-off
% Faults Detected
Fault Resolution
Manpower/Training Costs
Logistics Cost (Spares Provision)
Maintenance Support Costs
Test Equipment Complexity

2.1.2.8. DESIGN REVIEWS

PRELIMINARY DESIGN PHASE:
Informal as required in Activities 1 through 8
(9) Prepare System Hardware Design/ Interface Specifications

DETAILED DESIGN REVIEW:
Informal as required in Activities 1 through 4
(5) Prepare Final Hardware Design Description

Reliability
Maintainability
Availability
Life Cycle Cost
Produceability
Supportability
Testability
Quality Assurance

MTBF
MTTR
MTBR

Product Quality
Cost (Development/Testing)
% Problems Detected/ Corrected
Maintenance Support Costs
Manpower/Facilities Cost

I-13   INTENTIONALLY LET BLANK;
I-14   TABLES CONDENSED AND
I-15   REDUCED ON FOLDOUT PAGE I-12.

(Appendix I-A-1 through I-A-8 presents tutorials on each of these eight (8) tools/activities and examines some of the issues relevant to each of these tools/activities.)

In order for the tasks/activities (Appendix I-A-1 through I-A-8) to be properly evaluated, the contractor first needs to assess the proposed environment in which the emerging system is to become operational as well as the physical stresses that the product will encounter throughout its life cycle. Without these assessments, the product cannot be properly designed, integrated, and built with any degree of assurance that the desired integrity will be included in the fielded equipment.

The contractor needs to, as a minimum, conduct an environmental assessment based on the mission and environmental profiles provided by the Government as part of the Request for Proposal. System functional and environmental profiles need to be prepared on the basis of the total envelope of extgernal environments given by the mission profiles. Worst case environments need to be assessed and related to the stresses induced on avionics equipment need to be assessed and related to the stresses induced on avionics equipment and parts throughout the aircraft. These environmental analyses, when completed, can be translated into the design requirements for the component parts of the system during the preliminary and detailed design phases of the system development as it is being developed. The system designer and the system integrator need to work closely with the other vendors and/or subvendors in order to ensure that the outputs of the environmental assessment activities are applied consistently at all levels on an equal basis. In addition to the design assessment activities, it is necessary to assess/analyze all of the integration, mission, and maintenance concepts to determine the nature of the environments in which the avionics system will be operated, maintained, and otherwise provided for. In conducting the environmental assessments, the following environmental factors need to be considered:

- Electrical power distribution system (including emergency and abnormal power conditions) - (Reference MIL-STD-704)

- Environmental control system

- Mission induced environments - (Reference MIL-STD-810)

- Maintenance induced environments - (Reference MIL-STD-810)

- Shipping environment - (Reference MIL-STD-810)

- Shelf life - (Reference MIL-STD-810)

- Flight line environment.

Once these environmental assessments are completed, it is then possible for the system designer to analyze the referenced tools/activities, their impact on the various integrity attributes, and the potential change in cost that will result in the development phases as a function of applying the various tools/activities at the proper level called for by the environmental impact assessment.

For new sub-systems a stress analysis based on results of the integrated environment assessment needs to be completed. The stress analysis should be used as the basis of parts derating. The stress analysis should identify the maximum actual stresses (thermal, electrical, or mechanical) induced on a part in its application. Stress analysis in accordance with MIL-STD-785 Task 206 needs to be applied to all new sub-systems. This task should "examine the effects of parts/circuits, electrical tolerances, and parasitic parameters over a range of specified operating temperatures."[2] (Such parasitic parameters could include, for example, the inductance of wire-wound resistors or the parasitic capacitance of diodes and transistors.)

"There are essentially three stages in the life of a product, each having different rates and causes of failure. The Weibull curve (or 'bathtub' effect), which represents component failures over time, can also give an indication of product failures. These failures are caused by a combination of three basic failure mechanisms: early, stress-related, and wearout.

"Examples of early failures are bad connections due to poor solder joints or contamination, breaches in insulation, missing or incorrectly positioned parts, and internal opens and shorts in semiconductors. These problems surface during the infant stage, when parts are udnergoing their first stresses.

"Stress-related failures occur at any stage. Normal operating stresses will cause marginal components to fail at a fairly constant rate, but this rate can be minimized by designing circuits to operate well below component limits (derating).

"Wearout failures, caused by cumulative exposure to environmental changes and operating stresses, mark the beginning of the old age stage and the end of the product's useful life. At this point, failures start to increase dramatically."[3]

"A popular method of applying stress to finished products is static burn-in, where the units are placed on racks and turned on for a specified time period. This period, which can be hours, days, or weeks, is chosen to fail as many units as possible without taking an unreasonable amount of time to do it, since fewer units fail as time goes on.

"Burn-in triggers the early and stress-related failure types responsible for infant mortalities through the combined effects of time and temperature. Keeping power applied will usually cause internal temperatures to rise above nominal operating levels, especially if the units are stacked or placed in insulated racks. This elevated temperature increases the probability of marginal component failures; also, thermal gradients introduced along the chassis and PC boards as the unit heats up may identify some mechanical problems such as loose or inadequate mounting hardware."[3]

Typical problems induced by temperature stress include the following:

1. "Electronic components assembled on printed circuit boards (PCB's) impose loads on the solder joint, and thermal stresses may produce solder joint cracking. Heavy coats of conformal coating on even a stress relief bend can negate the beneficial effects of the bends.

2. "Transistors mounted on plastic spacers and coated with conformal coating will produce cracked solder joints in a few temperature cycles if the leads are not stress relieved. This problem arises because the coefficient of thermal expansion for plastics is about 8 to 30 times greater than Kovar transistor leads, or Dumet diode leads.

3. "Cordwood modules potted with a rigid, solid polyurethane or epoxy may produce cracked joints and even crush weak parts such as glass diodes on the very first application of a temperature cycle.

4. "Breakage of glass diodes can be expected if great attention is not given to the encapsulation material and the process."[4]

It has been found that the application of random vibration to avionic equipment is capable of precipitating failures in equipment that had previously undergone many hours of fixed-frequency sinusoidal vibration testing.[4] Typically, the failure mode is broken solder joints, loose connections, and broken wires due to insufficient stress relief, etc.

Vibration levels and duration, for stress screening purposes, can be found in the literature for many applications. "Various sources in the literature recommend random vibration levels of (0.04 - 0.045) g^2/Hz provided that the assembly/unit can withstand that level without damage.[5] The duration of the vibration is recommended as ten minutes in each of the unit's three axes." "The need for multiaxis excitation may be evaluated by determining the fallout per axis during intitial screening."[5]

Electrical stress tests can include "induced signal susceptibility tests, radio frequencies susceptibility tests (radiated and conducted), and emission of radio frequency energy tests."[6]

Other electrical stresses can include over/under voltage/frequency stresses, etc.

"A fairly new concept of stressing is cyclic burn-in, or power cycling. It can improve on the results of static burn-in by introducing additional stresses while cutting down on the total time needed for burn-in.

"Power cycling approximates mild temperature cycling on a micro level. It creates cyclic thermo-mechanical stresses across semiconductor junctions and ohmic contacts, forcing marginal devices to fail faster than they would with static burn-in. Longer cycling periods can cause mild mechanical flexing on a macro level, identifying such failures as cold solder joints, poor welds, and dielectric defects. Also, instruments with components unable to endure very high temperatures can be safely tested.

"Cyclic stressing approximates the real world environment better than static stressing does, because most instruments are turned on and off rather than left on continuously."[3]

An example of applying power cycling to a programmable power supply can be found in reference (3).

Based on the above discussions, it can be seen that the system designer not only has to be aware of the various tools and activities that impact the design/cost of the emerging system, but he must be aware of the environmental constraints and the physical stresses that the final product will see in its life cycle. It is these environmental constraints and physical stresses which when combined with the other design stage decisions (with respect to parts selection/handling criteria), that determine the success of the product in meeting the user's readiness/availability goals as well as the longer term logistics/maintenance issues which impact the economic life costs of the system. These decisions must be made at the Design Stage and carried out throughout the integration, manufacturing, and deployment phases of the product's life cycle.

2.1.3 Contractor's Prototype Development Phase

The activity in this phase centers on assembling a "laboratory" prototype using available production techniques, available parts and components and production personnel. The technology, components, and personnel used in assembling the prototype should be representative of the resources to be used in production in order to assure that precipitated failures, due to testing, will be representative of the actual production process. If, however, differences are introduced, such as nonstandard or "replacement" parts (due to unavailability of the specified parts), these differences must be documented and any variances noted, along with an estimate of the effect of the differences from a testing perspective.

During this phase the assembled prototype needs to be actively stressed/stimulated using appropriately specified stress screens (AC power, thermal, vibration, etc.) to induce failures and discover design deficiencies that have "as-yet" been undetected by the failure modes and effects (FMEA) analyses and the fault tree construction. It is important that the stress screens are properly designed and implemented (a) to detect-analyze-and-fix (TAF) design errors, (b) to replace marginal parts and components with "better" quality parts, and (c) to identify and fix manufacturing processes that contribute to failures. The costs associated with changes at this point are more expensive than if they had been anticipated at an earlier point (i.e., PDR or CDR), however, it is significantly cheaper and easier to correct deficiencies at this point than after production has begun.

Screening tests are employed in order to eliminate incipient failures from critical assemblies that comprise hardware systems during the manufacturing process (Reference Appendix I-A-4). The best screens are those which remove inferior assemblies and reduce the defect rate by methods of stress application. The term "screening" can be said to mean the application

to an assembly of a stress test, or other tests, which can reveal inherent weaknesses (and thus incipient failures) without destroying the integrity of the assembly. Thus, the purpose of reliability screening is to compress the early failure period and reduce the failure rate to acceptable levels as quickly as possible. However, a thorough knowledge of the equipment to be screened and the effectiveness and limitations of the various tests is necessary in order to produce a useful and reliable screening procedure for the component module or subassembly under test.

Theoretically, screening can be optimized (in terms of extent, duration and assembly level) if the following parameters are known:

1. The latent failure modes existing in a sample population;

2. The stresses and indicators useful in detecting these modes;

3. The costs involved in any screening activities.

If these data are known, it would be possible to select the proper sequence of screens such that a given test would not duplicate the results of a previously performed test. Unfortunately, in most cases, the cost and time factors involved in assimilating failure mode data are too high, or the data are not good enough to produce confident extrapolations of current results to future production. Thus, the normal procedure is to continually adjust the screening processes, depending on the failure modes which occur, and introduce tests or controls which would reduce cost and alleviate possible failure mode problems.

Since testing involves the application of stress test, or tests to hardware on a 100 percent basis for the purpose of revealing inherent part, module subassembly and workmanship defects without weakening or destroying the product. Screens are designed to detect and eliminate defects that would not be detected ordinarily by normal quality inspections and tests.

Screen tests can be applied at various assembly levels (e.g., part, assembly board, or at the system level). However, some part defects are more easily detected as part of an assembly board test. This is particularly true of drift measurements and marginal propagation delay problems. Assembly defects, such as cold solder joints, missing solder joints, and connector contact defects can only be detected at the board or product level. The higher the assembly level, the lower the tolerance for stress and, thus, the lower the stress that can be acceptably applied. As a general rule, screens for known latent defects should be performed as early in the assembly process as is possible--at the time when higher stress levels and more cost effective screens can be applied.

Temperature cycling is a highly effective stress test that can be used to detect workmanship defects as well as intrinsic part defects at both the assembly board and equipment level. The number of intrinsic part defects found at the board level is dependent on the extent of the screening applied at the part level. Experience has shown that significant part defects have been found to be present at the board and higher levels of assembly even when the parts have been 100% screened. Therefore, temperature cycling at the assembly board level is performed to reveal:

- PCB defects (including delamination, fracture, and insulation cracking)

- Part/board bond separation

- Solder problems (cracking, opens, etc.)

- Part defects (due to handling, etc.)

- Tolerance drift (analog).

The number of temperature cycles required to precipitate defects is known to be dependent upon board density and part technology. The number of failures should be recorded for each cycle and analyses should be performed on failed parts/PC boards to determine the underlying failure mechanisms, as well as the possibility of earlier detection and the application of more stringent inspection and screens at the part level.

Stress screen tests at the equipment level are necessary, even if the part and assembly board screen tests had eliminated all defective parts and board defects, because the assembly of the remaining parts and the boards into the larger assemblies and into the final equipment cannot be assumed to be accomplished without incurring defects. Good parts can be damaged in assembly, workmanship errors can occur, and design defects can be either present or induced. Typical reliability and quality defects found in equipment have been overstressed parts, improper solder joints, cracked wires due to insufficient stress relief, and, despite quality control inspections, equipment have been produced with parts missing. Equipment level stress screening is used to induce or detect these defects prior to production.

The application of screening techniques have proven to be cost effective for both electronic and mechanical assemblies resulting in a reduction of in-process defects and thus, improved reliability in the final product. For example, the following sequence of events shows how some of the failure mechanisms are induced or detected in a power supply which was stress tested at the prototype level.*

"A development team has just finished the lab prototype for a new programmable power supply. It works fine under ambient conditions, and now they want to stress it. After evaluating their design they have come up with the following stress test, which they apply with a full rated load across the output of the power supply:

- Apply twenty 30-second cycles (20% duty cycle) to create thermal junction gradients within the IC's in the control circuitry. The short duty cycle keeps external component temperatures at ambient.

- Turn on power for 30 minutes, with the unit in an insulated box, to reach 60 degrees C. This stresses the mechanical components.

- Apply twenty 30 second cycles (80% duty cycle) to test the input current limiting circuitry. The long duty cycle ensures that the temperature remains high.

- Turn off power for 40 minutes to allow the unit to cool to 25 degrees C. This stresses the mechanical components again.

- Repeat this sequence until the unit fails.

"The unit fails on the fourth run during the high temperature (80% duty cycle) sequence. Analysis reveals that a power transistor can't tolerate the excessive inrush currents at high temperatures. They decide to use a higher power transistor with better heat sinking. To make sure the problem is solved, the high temperature cycling is increased from 20 to 30 cycles.

"Over the next week, four failures result in some modification of the control circuitry to make it less sensitive to high temperatures. These modifications are tested by increasing the heating time from 30 to 60 minutes.

"Eventually everyone is satisfied, and the unit goes into production. The modified strife test is now:

- twenty 30 second cycles (20% duty)

- power on for 60 minutes

- thirty 30 second cycles (80% duty)

- power off for 40 minutes

The production prototypes go through this sequence for four days. They are found to fail during the temperature excursions due to three points which are poorly soldered. A process correction is made, then the units are released. During regular production, each unit is stressed four times, for a total test time of eight hours and 20 minutes."[3]

In addition to the successful completion of a prototype model, this phase also results in the completion of the Reliability Growth Testing which is one of the main objectives of test prototype testing stage as it exists in current practice today.

"The objective of a reliable growth process, especially a reliability growth test, is to achieve acceptable field use reliability. Achievement of acceptable reliability is dependent on the extent to which testing and

other improvement attributes have been used during development to "screen out"
design and fabrication flaws, and on the rigor with which these flaws are
analyzed and corrected. The primary objective of growth testing is to provide
methods by which hardware reliability development can be dimensioned, disci-
plined, and managed as an integral part of overall development. Reliability
growth testing also provides a technique for extrapolating the current reli-
ability status (at any point during the test) to some future result. In addi-
tion, it provides methods to assess the magnitude of the test-fix-retest
effort prior to the start of development, thus allowing tradeoff decisions.

"For electronic systems, the model most commonly used for reliabil-
ity growth testing is the reliability growth plot in Figure I-2.1.3-1.
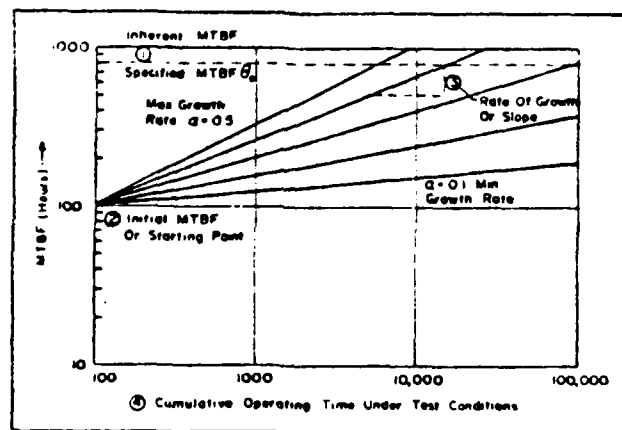
FIGURE I-2.1.3-1.   Reliability Growth Plot

"Essentially, this model provides a deterministic approach to reli-
ability growth such that the system MTBF versus operating hours falls along a
straight line when plotted on log-log paper. That is, the change in MTBF
during development is proportioned to $T\alpha$. Where T is the cumulative oper-
ating time and α the rate of growth corresponding to the rapidity with which
faults are found and changes made to permanently eliminate the basic causes of
the fault observed.

"The value of the parameter α can vary between a minimum of 0.1
(which can be expected in a program where no specific consideration is given
to reliability) and a maximum of 0.5 (where an aggressive reliability program

with management support is implemented). In the cases of minimum growth rate, growth is largely due to a solution of problems impacting production, and from corrective action taken as a result of user experience. Maximum growth rate occurs due to a formal stress oriented test program, designed to aggravate and force defects, and vigorous corrective action. For example, Figure I-2.1.3-1 shows a product with an MTBF potential (inherent reliability) of 1000 hours and an initial MTBF (starting point) of 100 hours. Thus, at the minimum growth rate (α) of 0.1, the achievement of an MTBF of 200 hours (double the initial MTBF) requires 100,000 hours of cumulative operating time. This is the case when no specific attention is given to reliability growth. However, if the growth rate can be accelerated to the maximum value of 0.5 (by growth testing and formal failure analysis activities), then only about 400 hours of cumulative operating time is required to achieve an MTBF of 200 hours."[7]

The progress of the growth testing needs to be tracked, and logs and data forms maintained that record the number of units undergoing test, test time accumulated, failures, corrective actions, level of reliability, and, finally MTBF achieved during the specified test time period.

A method for reporting, analyzing, and initiating corrective actions for all failures that occur during reliability growth testing of the prototype needs to be established as part of the reliability testing plan. This method which results in a formal, closed-loop failure analysis program is known as Failure Reporting, Analysis and Corrective Action (FRACA).

"The FRACA program is a key element in "failure recurrence control" for newly developed and production equipment. The program requires written procedures which describe the sequence of events that occurs upon detection of a failure. These include: methods, personnel responsibilities, scheduling, depth of analysis, reporting forms, and describe the applicability of the FRACA to reliability growth, reliability and maintainability demonstration, production screening, and acceptance testing.

"Upon discovery of a failure, the test operator should initiate a failure report. Failures are defined, in general, as any deviation from the acceptable value called out in the applicable test procedure. Failure analysis must be performed on failed assemblies and parts to determine root causes and underlying mechanisms of failure. All failures must be reported and the results of all failure analyses must be documented in a form designed for this purpose. The form should include entries for identification of data, conditions under which failure occurred, operating parameters, references to the applicable test plan and complete details leading up to or surrounding the failure incident.

"A suggested form (1) failure reporting, (2) failure analysis, and (3) corrective action is shown in Figure I-2.1.3-2. The form is, for the most part, self-explanatory. The cause of failure, in so far as it is possible to be determined, should be entered in the space marked "analysis." Corrective measures should be recommended that may eliminate or minimize the failure mechanism and should be described in the appropriate space. These measures could involve:

MALFUNCTION FAILURE REPORT

System Name _____   Date of Occurrence _____

Project Number _____   Operating Time _____

Equipment Name _____	Assembly Name _____	Part Name _____	Time To Failure _____
Eqpt. No. ____ Serial No. ____	Assy No. ____ Serial No. ____	Part No. ____ Serial No. ____	Elapsed Time _____
			Repair Time _____

Failure Discovered During:

		Test Procedure No.	Test Procedure Paragraph No.
R Growth	☐	____	____
R Demonstration	☐	____	____
M Demonstration	☐	____	____
Production Screening	☐	____	____
Acceptance	☐	____	____

Symptoms or Description of Malfunction/Failure

| Signature | Date |

FAILURE ANALYSIS REPORT

Description of Analysis Approach, Techniques, Results and Conclusions   (Use Additional Sheets if Necessary)

Parts/Assemblies Replaced

Part No. _____ Mfg. _____ S/N Date _____
_____ Mfg. _____ S/N Date _____
_____ Mfg. _____ S/N Date _____

Assy No. _____ Mfg. _____ S/N Date _____
_____ Mfg. _____ S/N Date _____
_____ Mfg. _____ S/N Date _____

Other _____ Mfg. _____ S/N Date _____
Replacements _____ Mfg. _____ S/N Date _____
_____ Mfg. _____ S/N Date _____

| Corrective Action To Be Requested ☐ Yes ☐ No | Signature | Date |

CORRECTIVE ACTION

To: _____ Dept. _____ Date of Request _____

Description of Problem

Recommended Action

| Signature(s) | Date | Signature(s) | Date |

Action Taken (Describe)

Follow-Up Action Required ☐ Yes ☐ No

Signature(s) _____ Date _____
_____ _____
_____ _____

ECN or ECP No. _____ Approval _____ Date _____

FIGURE I-2.1.3-2.   Failure Reporting, Analysis, and
Corrective Action Form (Reference 7)

1. System/equipment redesign.

2. Part selection criteria.

3. Part derating criteria.

4. R growth and demonstration.

5. Special screenings to weed out specific failure mechanisms.

6. Special in-process fabrication inspections and tests.

7. Special reliability assurance provisions."[7]

Failure Diagnosis[8]

After a failure has been determined to have occurred during stress screening of the prototype, it is necessary to determine how the failure occurred and to identify the failure mechanism responsible for the failure. There is no established procedure for conducting the analysis of the failed part, component, or process; however, nondestructive tests should be performed first in order to keep the samples intact as long as possible. Nondestructive tests include:

- Low-power optical magnification

- Dye penetration tests

- Magnetic particle tests

- Thermographic, ultrasonic, eddy-current techniques/tests

- Physical property measurements.

After completion of the nondestructive tests, it is then possible to cut or otherwise disturb part(s) in order to characterize the chemical, structural, and mechanical failure mechanisms that might have caused the failure. Investigative techniques and devices used in "destructive" tests include:

- Electronic optical equipment

- Scanning electron microscopes

- Energy dispersive spectroscopy

- Electron probe analysis

- Chemical analysis

- Composition analysis.

Both the nondestructive and destructive testing will identify the mechanisms of failure and if a consistent pattern is found in a part or process, the parts manufacturer or the manufacturing organization can be notified and the part/process modified or a new part selected or a process changed in order to meet the reliability goals established in the system specification or design documents that resulted in the production of the prototype. Table I-2.1.3-1 presents the Inputs/Outputs, Tools and Integrity parameters, criterion and measures associated with the final stage of the design phase which is the assembly or buildup of the prototype subassemblies and or systems.

At the conclusion of the Contractor's Prototype Development Phase, the emerging system has been defined in terms of its hardware considerations, the initial concepts which guided the design have been proved and the hardware system is ready to be mated with the system software in the integration stages of development, as well as other hardware components (cables, connectors, other subsystems, etc.) for functional testing and interface compatibility evaluation. It is also assumed that the reliability/maintainability predictions have been initially validated and that the product, when integrated and properly manufactured, will meet the reliability/maintainability/testability and availability goals without the need for extensive redesign efforts.

TABLE 1-2.1.3-1. PROTOTYPE DEVELOPMENT PHASE CHARACTERISTICS AND INTEGRITY ATTRIBUTES

Activity	Sub-Activity	Input	Output	Tools	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.4 Contractor's Prototype Development Phase	Assemble Prototype	Hardware CDR Results Hardware Test Plans Component/Parts Test Plan	"As-Built" Description	People Parts Process	Reliability Testability Producibility Manufacturing Quality	MTBF MTTR MDT	Final Inspection Form/Fit/ Function
	Stress Screen	Stress Test Characteristics Known Latent Failure Modes	Final Stress Screen(s)	Stress Screen Apparatus and Equipment Logs/Test Results	Reliability Testability	MTBF MTTR MDT	Failures Failure Rates
	Reliability Growth Test	Target MTBF Minimum Acceptable MTBF Starting MTBF Min/Max Expected Growth Rate	Production MTBF	Data Acquisition system Logs/Test Results	Reliability Availability	MTBF	MTBF Increase Toward Goal
	Failure Reporting, Analysis & Corrective Action	Failed Component/Process	Correction Action	Forms Checklist	Reliability Repairability Producibility	MTBF MTTR MDT	Time Cost
	Failure Diagnosis	Failed Component	Physics of Failure Recommended Corrections	Nondestructive Tests Destructive Tests	Reliability Producibility Availability	MTBF MTTR	Time Cost Failure Rate Decrease Toward Goal

2.1.4 References

1. The Avionics Integrity Program (AVIP), Dickman, T. J., and Cheshire, L. F. (Major), Federal Acquisition Research Conference/Symposium, December 1983.

2. MIL-STD-7853, Electronic Parts/Circuits Tolerance Analysis, September 15, 1980.

3. Testing for Equipment Reliability with AC Power Cycling", Petersen, J., Evaluation Engineering, pp. 70-73, April 1983.

4. Navy Manufacturing Screening Program, NAVMAT-P-9492, May 1979.

5. Environmental Stress Screening, ESD Draft, United States Air Force, May 1982.

6. Validation of Digital Systems in Avionics and Flight Control Applications, DOT/FAA/CT-82/115, Hitt, E. F., et al., July 1983.

7. Reliability and Maintainability Implementation Notebook, Federal Aviation Administration (Airway Facilities Service), Volume 4, 1981.

8. Failure Analysis - Aims, Approaches, Applications, Wood, R. A., Battelle Technical Inputs to Planning/Report No. 36, Battelle Memorial Institute, Columbus, Ohio 43201.

2.2 SYSTEM INTEGRATION PHASE ACTIVITIES ANALYSIS

The start of this system integration phase often overlaps final activities in the design phase. The completion of the system integration phase as described in this report overlaps nearly all the system full-scale development (FSD) activities.

This section of this report primarily deals with the system integration activities related to the integration and test of the prototype system with the necessary feedbacks which result from the test phase. The activities during this system integration phase do not include the production manufacturing activities which are discussed in following sections of this report.

It is assumed that prior to beginning the system integration phase activities, the system functions have been fully defined and allocated between hardware, software, and the human user. It is further assumed that the hardware design reviews, including preliminary design and critical design have taken place. It is assumed that the build of the prototype hardware and the associated testing have been completed.

The activities described in this system integration phase assume the software is developed by the system integrator. If not, both the preliminary and critical design reviews of the software may have already been held. Prior to initiation of the system integration phase, it is assumed that those responsible for system integration have participated in the design phase activities related to the development of system hardware and system software interface specifications. The system hardware interface specifications should describe all hardware interfaces between subsystems. This interface would include not only mechanical but also electrical interfaces. The electrical interfaces would be described to the level at which each pin in each connector has each signal defined in terms of its electrical characteristics as well as any associated timing characteristics in the case of digital signals.

The system software interface specification must describe in detail the requirements for all data transmitted between digital subsystems. The format of each word and, in multiple word messages, the format of each message shall have been totally specified. If the data transmission rates are on a synchronous basis, the transmission rate shall be specified. If a command response protocol is used, in which the address and subaddresses are used for communication, rather than a broadcast protocol, the transmit/receive addresses and subaddresses of each message (or word in single word messages) is given. This system software interface specification serves as a basic software interface control document and should be under configuration control. Any data transmission between subsystems other than those prescribed in the software interface specification should be invalid.

With this background, those activities normally considered to take place during this system integration phase will be analyzed in the following sections of this report. For each activity, a number of subactivities are identified. The respective inputs and outputs of each activity, and tools used in that activity, will be documented in a table for each activity. In

addition, the system integrity parameters, criteria, and measures for activity will be included in a separate table.

Figure 2.2-1 depicts a representative overall sequence of activities for the system integration phase. There are decision points associated with nearly every activity and to include the feedback loops due to these decisions would make the figure more complicated. Therefore, these feedback loops are not shown.

2.2.1 Analyze Avionics Design Specifications (Activity 2.1)

This task consists of many subactivities that are shown in Table 2.2.1. The inputs to this task are the system specifications and each of the LRU specifications as well as the hardware interface control documents and the system software interface specification. If the avionic software is not being developed by the system integrator, then the software specification should also be made available for analysis.

The purpose of the analysis is to extract that information required to develop the avionics integration support facility, avionics airborne software, and the subsequent integration and testing of the pre-production proto- type avionics system.

This analysis can be performed manually and manual documentation methods used to compile the results. An alternative, which should result in a system with higher integrity, is to document the results of the analysis in a software data base system which could be accessed and used throughout the remainder of the system life cycle. This would assure that only a single data base is being used and reduce problems of design and development personnel maintaining manual documents which may not be current. As shown in Table 2.2-2, the primary integrity measures are the man-hours, computer time, and calendar time. The use of data base software should result in a significant savings in both the man-hours and the calendar time at the expense of some computer time.

The outputs of this activity are an avionics specification analysis report and the data contained in the data base if the data base software is utilized.

2.2.2 Establish Avionics Integration Support Facility (AISF) Requirements (Activity 2.2)

The inputs to this activity are the avionics specifications and analysis report and the data in the data base.

The contents of the avionics specifications and analysis report and data base should be analyzed to determine the hardware, software, and human resources required to develop and operate the avionics integration support facility. Analysis must concern itself with determining the physical
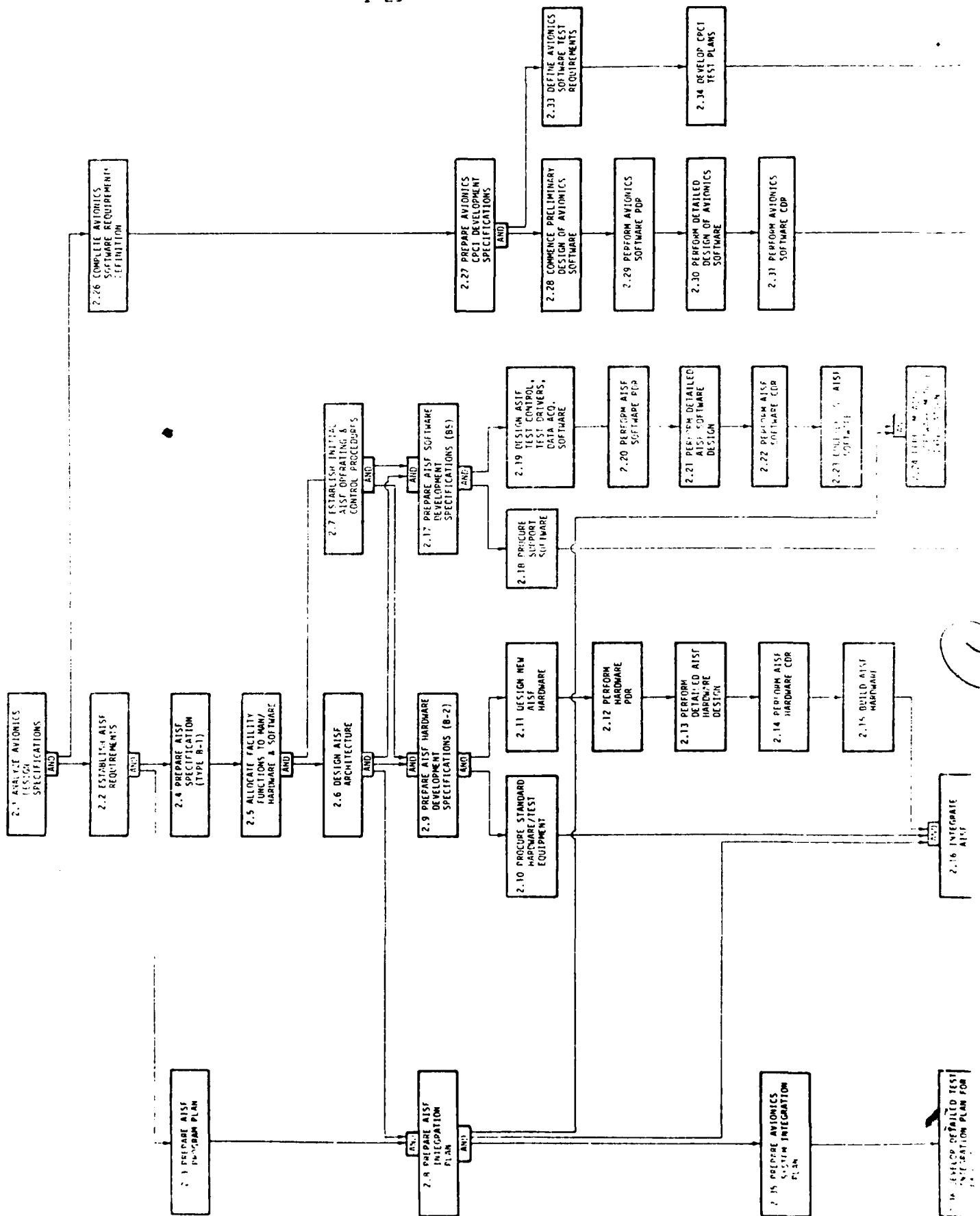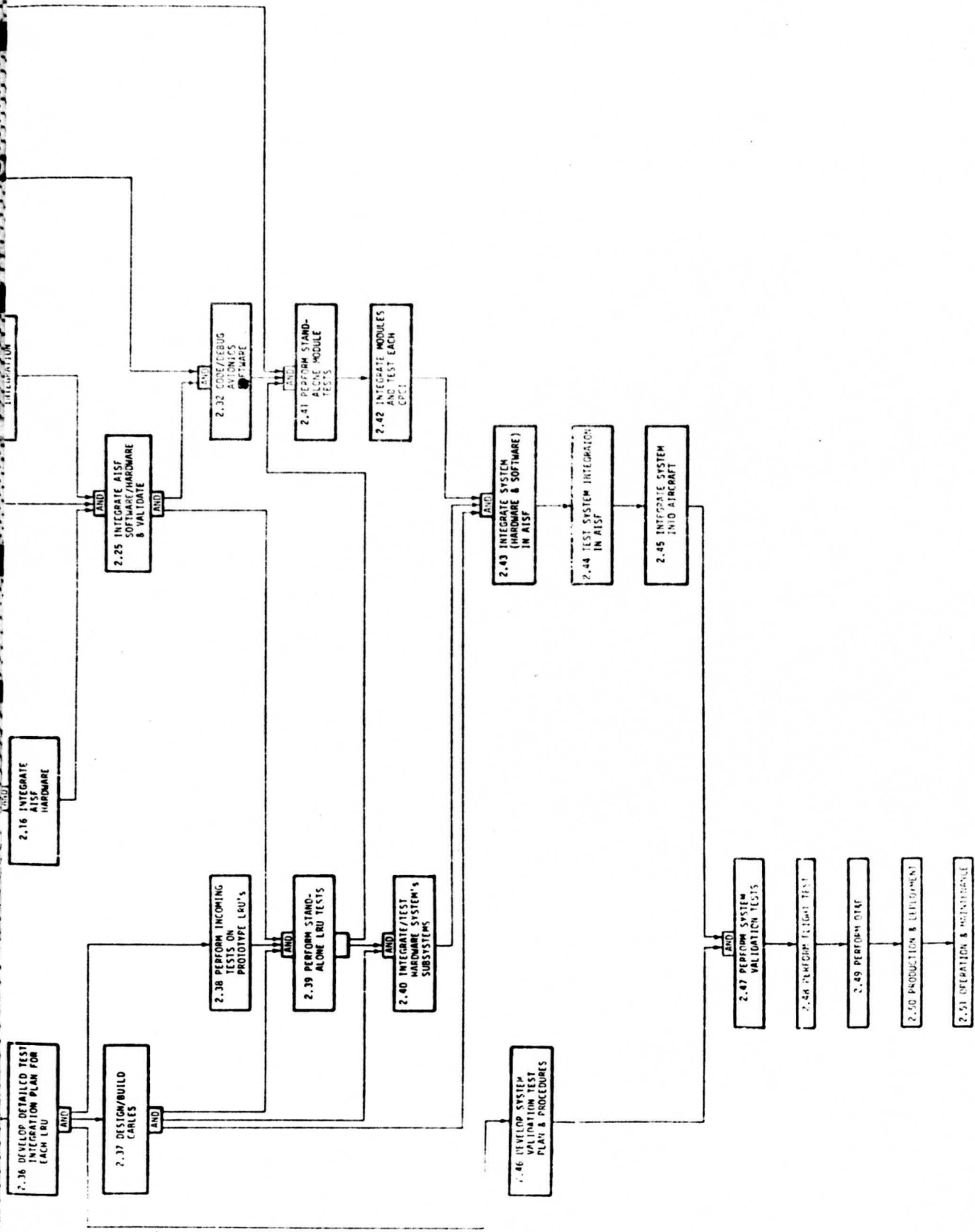
FIGURE I-2.2-1. SYSTEM INTEGRATION PHASE ACTIVITIES

2.16 INTEGRATE AISF HARDWARE

2.25 INTEGRATE AISF SOFTWARE/HARDWARE & VALIDATE

2.32 CODE/DEBUG AVIONICS SOFTWARE

2.41 PERFORM STAND-ALONE MODULE TESTS

2.42 INTEGRATE MODULES AND TEST EACH CPCI

2.43 INTEGRATE SYSTEM (HARDWARE & SOFTWARE) IN AISF

2.44 TEST SYSTEM INTEGRATION IN AISF

2.45 INTEGRATE SYSTEM INTO AIRCRAFT

2.36 DEVELOP DETAILED TEST INTEGRATION PLAN FOR EACH LRU

2.37 DESIGN/BUILD CABLES

2.38 PERFORM INCOMING TESTS ON PROTOTYPE LRU's

2.39 PERFORM STAND-ALONE LRU TESTS

2.40 INTEGRATE/TEST HARDWARE SYSTEM's SUBSYSTEMS

2.46 DEVELOP SYSTEM VALIDATION TEST PLAN & PROCEDURES

2.47 PERFORM SYSTEM VALIDATION TESTS

2.48 PERFORM FLIGHT TEST

2.49 PERFORM OT&E

2.50 PRODUCTION & DEPLOYMENT

2.51 OPERATION & MAINTENANCE

TABLE 2.2-1. INTEGRATION PHASE ACTIVITIES, DOCUMENTATION, AND TOOLS (Page 1 of 5)

Activity	Subactivity	Inputs	Outputs	Tools
2.1 Analyze Avionics Design Specifications	Analyze System Specification (Type A)* Analyze LRU(s) Specifications (Types B1, B2)* Analyze Software Specifications (Type B5)* Analyze Hardware Interface Control Documents (ICD) Analyze System Software Interface Specification	System Specification LRU(s) Specifications Software Specifications Hardware ICD System Software Interface Specification	Avionics Specification Analysis Report (ASAR) Data in Database	Database Software
2.2 Establish Avionics Integration Support Facility (AISF) Requirements	Analyze ASAR and Database Prepare Requirements Document	ASAR Data in Database	AISF Requirements Document (AISFRD) AISF Data in Database	Database Software
2.3 Prepare AISF Program Plan	Develop Work Breakdown Structure (WBS) Develop Task Descriptions Develop Schedule Determine Manpower/Budget	AISFRD	AISF Program Plan	Program Management Software
2.4 Prepare AISF Specification (Type B1)	Analyze AISFRD and Database Prepare Specification for Publication	AISFRD AISF Data in Database	AISF Specification (Type B1)	Word Processing System Data Base Software
2.5 Allocate Functions to Man/Hardware and Software	Analyze Tasks Allocate Tasks to Man/Machine Allocate Machine Tasks to Hardware and Software	AISFRD AISF Data in Database AISF Specification	AISF Function Allocation Report (FAR)	Word Processing Data Base Software
2.6 Design AISF Architecture	Analyze Reliability/Maintainability Analyze Facility Usage	AISF FAR Database AISF Specification AISFRD	AISF Architecture Report	Reliability Analysis Program Data Communication Analysis Program
2.7 Establish Initial AISF Operating and Control Procedures	Analyze Existing Facility Operating and Control Procedures Define User Interface Requirements	Architecture Report AISFRD and Specification AISF FAR AISF Data in Database	AISF System Operating/Control Procedures (SOCP) Report	Work Processing System Data Base Software
2.8 Prepare AISF Integration Plan	Analyze Architecture Report Analyze Schedules Develop Integration Sequence and Procedures	AISF Program Plan AISF Architecture Report AISF Specification	AISF Integration Plan	Program Management Software Word Processing System Data Base Software
2.9 Prepare Hardware Development Specification (d2)	Prepare Specifications for Standard Hardware and Test Equipment Prepare Development Specification for Hardware to be Designed	System Specification AISF Specification LRU(s) Specifications Hardware ICD System Software Interface Specification	Standard Hardware Specifications Test Equipment Specifications Hardware Development Specifications	Word Processing Software Data Base Software

*As defined in MIL-STD-490.

TABLE 2.2-1. INTEGRATION PHASE ACTIVITIES, DOCUMENTATION, AND TOOLS (Page 2 of 5)

Activity	Subactivity	Inputs	Outputs	Tools
2.10 Procure Standard Hardware/ Test Equipment	Prepare Procurement Packages Issue RFQ Award Contract	Standard Hardware Specifications Standard Test Equipment Specifications	Procurement Packages Contract	Word Processing System Data Base Software
2.11 Design New AISF Hardware	Prepare Procurement Issue RFP/Evaluate Proposal/Award Contract	Hardware Development Specifications Proposal Contract	Procurement Packages Proposal Contract	Computer Aided Design (CAD) System Qualified Parts Database Reliability Analysis Program Parts Derating Program
2.12 Perform Hardware Preliminary Design Review	Review Performance Estimate Review Reliability Review Interfaces Review Parts List	Hardware Design Description Document Hardware Development Specifications Hardware ICD System Software Interface Specifications Data in Database	Discrepancy Reports	PDR Checklist Database Software
2.13 Perform Detailed AISF Hardware Design	Breadboard Circuits Evaluate Performance Screen Sample Parts Update Specifications Update Drawings	Discrepancy Report (Plus all of 2.12 Inputs) Sample Parts	Updated Specifications and Drawing	CAD System Qualified Parts Database Environmental Test Facility Screening Test Facility
2.14 Perform AISF Hardware Critical Design Review	Review Performance Review Recommended Updates to Preliminary Design Update Specifications and Drawings	All 2.12 Inputs Updated Specifications/Drawings Performance Test Result	Approved Changes Action Items Updated Specifications and Drawings	CDR Checklist Database
2.15 Build AISF Hardware	Select Screened Parts "Build to Print" Inspect and Test Card Integrate Cards into Boxed Test	Updated Specifications and Drawings Screened Parts	AISF Hardware "As Built" Drawings	Prototype Manufacturing Facility Manufacturing Test Equipment Environmental Test Facility
2.16 Integrate AISF Hardware	Integrate Facility Computers Integrate Test Equipment Verify Form/Fit/Function Verify Interfaces	AISF Integration Plan/Procedures AISF Hardware/Test Equipment AISF Cables AISF Facility	Integrated and Tested AISF Hardware	Test Equipment Test Software Drivers
2.17 Prepare AISF Software Development Specifications (Type B5)	Define Software Functions Required Define Software Modules Define Software Interfaces Prepare Software Specifications	AISF Specification AISF Function Allocation Report AISF Architecture Report AISF SOCP Report	AISF Software Development Specifications (B5) • Software Development Support • Simulation • Test Drivers • Data Acquisition/Reduction	Word Processing System Data Base Software Requirements Analyzer

TABLE 2.2-1. INTEGRATION PHASE ACTIVITIES, DOCUMENTATION, AND TOOLS (Page 3 of 5)

Activity	Subactivity	Inputs	Outputs	Tools
2.19 Design AISF Test Control, Test Drivers, Data Acquisition Software	Design AISF Executive Design Test Control Software Design Test Drivers Design Simulation Support Design Data Acquisition/Reduction Software Conduct Design Walkthrough	Software Development Specifications	Software Design Description Reports	Functional Simulator
2.20 Perform AISF Software PDR	Determine Consistency of Design with Requirements Determine Adequacy of Test Requirements	AISF Software Development AISF Software Design Description Reports (DDR) AISF Software Test Requirements Document (TRD)	AISF Software Discrepancy Reports	Database Software Walkthrough Checklist
2.21 Perform Detailed AISF Software Design	Prepare Detailed Design Document and Draft of AISF Software Product Specifications and Test Plans/Procedures	AISF Software Discrepancy Report Inputs of Activity 2.20	Detailed Design Document Draft AISF Draft AISF Software Product Specifications Draft Test Plans/Procedures	Word Processing System Data Base Software
2.22 Perform AISF Software CDR	Determine Consistency of Design with Requirements Determine Consistency of Test Plans/Procedures with Test Requirements	Detailed Design Document Draft-AISF Software Product Specification and Test Plans/Procedures AISF Software Development Specifications	Approved Changes Action Items AISF Software Design Baseline Documents	Database Software Software Engineering Verifier
2.23 Code/Debug AISF Software	Code Modules Debug Modules Perform Stand Alone Module Tests	AISF Software-Develop Specification, Draft Product Specification, Design Description Documents, Test Plans/Procedures	Coded/Debugged Modules Code/Debug Status Reports Updated Software Database	Compiler, Assembler, Linker, Loader, Editor Static Analyzer Dynamic Analyzer
2.24 Perform AISF Software Module Integration	Integrate and Test Modules in Sequence Acquire Data Analyze Data Correct as Required	Coded/Debugged Modules Test Driver Software	Module Integration Test Report CPCI Source/Object Code	Database Software Automated Verification System Instrumentation Software
2.25 Integrate AISF Software/Hardware and Validate	Integrate and Test AISF Software with AISF Hardware Acquire Data Analyze Data	CPCI Source/Object Code Test Integration Software	AISF System Integration Report	Test Case Generator Software
2.26 Complete Avionics Software Requirements Definition	Analyze System Specification Verify Software Interface Specification Analyze Functions Allocated to Software Review User Requirements	System Specification Avionics System Operating and Control Procedures	Avionics System Software Development Specification Software Development Plan	Requirements Engineering Methodology Software

TABLE 2-2-1. INTEGRATION PHASE ACTIVITIES, DOCUMENTATION, AND TOOLS (Page 4 of 5)

Activity	Subactivity	Inputs	Outputs	Tools
2.27 Prepare Avionics CPCI Specifications	Determine Software Functions for Each Computer; Define Software Modules; Define System Software Interfaces; Prepare Specification	Avionics System Software Development Specification; Software Development Plan	Computer Program Configuration Item (CPCI) Development Specification(s); System Software Interface Specification	Word Processing Systems; Data Base Software; Software Specification Language
2.28 Commence Preliminary Design of Avionics Software	Design Modules; Document Design; Conduct Design Walkthrough	CPCI Development Specifications; Software Development Plan; System Software Interface Specification	Software Design Description Report	Functional Simulator; Existing Software Modules; Source Code; Program Design Language
2.29 Perform Avionics Software PDR	Determine Consistency of Design with Requirements; Determine Adequacy of Test Requirements; Determine Adequacy of Support Tools	CPCI Development Specifications; Software Design Description Report; Software Test Requirements Document; Software Development Support Tools	Software PDR Report	Database Software; Walkthrough Checklist
2.30 Perform Detailed Design of Avionics Software	Prepare Detailed Design Document and Draft of Avionics Software Product Specifications, and Test Plans/Procedures	Software PDR Report; Inputs of Activity 2.29	Detailed Design Document; Draft Avionics Software Product Specifications; Draft Test Plans/Procedures	Word Processing System Database Software; Program Design Language (ADA)
2.31 Perform Avionics Software CDR	Determine Consistency of Design with Requirements; Determine Consistency of Test Plans/Procedures with Test Requirements	Detailed Design Document; Draft-Software Product Specification and Test Plans/Procedures; Software Development Specifications	Approved Changes; Action Items; Software CDR Report; Software Design Baseline Documents	Database Software; Software Engineering Verifier
2.32 Code/Debug Avionics Software	Code Modules; Debug Modules	Avionics Software Development Specification; Draft Avionics Software Product Specifications; Software Design Baseline Documents	Coded/Debugged Modules; Code/Debug Status Report; Updated Software Data Base	ADA Compiler; Assembler; Linker, Loader; Editor
2.33 Define Avionics Software Test Requirements	Define Test Approach; Define Test Responsibilities; Define Software Metrics/Standards; Define Change Proposal Procedure; Define Test Report Requirements	System Specification; CPCI Development Specifications; Updated Software Database	Test Requirements Document	Software Test Guidelines
2.34 Develop CPCI Test Plans	Develop Stand-Alone Test Plan; Develop Software Integration Test Plan; Develop Flight Software Test Plan	System Specification; CPCI Development Specifications; Test Requirements Document	Detailed Test Plans and Procedures (See Figure 2.2-3)	Software Test Guidelines
2.35 Prepare Avionics System Integration Plan	Define Sequence of Integration Steps; Define Sequence of Tests for Step; Define Equipment Required; Define Software Required	System Program Plan; AISF Integration Plan; System Specification; LRU Specifications; Software Specifications	Avionics System Integration Plan	Word Processing System; Data Base Software

TABLE 2.2-1. INTEGRATION PHASE ACTIVITIES, DOCUMENTATION, AND TOOLS (Page 5 of 5)

Activity	Subactivity	Inputs	Outputs	Tools
2.36 Develop Detailed Test/Integration Plan for Each LRU	Develop Test Plan for Each Integration Step Sequence Develop Detailed Test Procedures	LRU Specifications System Specification Software Specifications Avionics System Integration Plan	Detailed Test Plans Detailed Test Procedures	Sample Test Plan Outline (Table 2.2.3) Sample Test Procedure Outline (Table 2.2.4) Word Processing System
2.37 Design/Build Cables	Design Avionics Cables Design AISF Interface Cables Procedure Parts Build/Test Cables	Hardware ICD LRU Specifications System Specification AISF Hardware Product Specification	Avionics Cables AISF/Avionics Interface Cables	CAD System Qualified Parts Database Parts Derating Program Database Software
2.38 Perform Incoming Tests on Prototype LRUs	Perform Inspection Perform Acceptance Test	Prototype LRUs LRU Detailed Test Plan/Procedures	Accepted LRU Incoming Test Report Updated Hardware Data Base	Test Plan/Procedures Checklist Acceptance Test Equipment
2.39 Perform Stand Alone LRU Tests	Conduct Stand Alone Tests Conduct Performance Verification Perform Environmental Qualification Test	Detailed Test Plan Detailed Test Procedures Accepted LRU	LRU Stand Alone Test Report Updated Hardware Data Base	Computer Controlled Test Equipment Software Test Drivers Environmental Test Chambers
2.40 Integrate/Test Hardware Systems' Subsystems	Review Test Sequence for LRU Set Up Test Equipment Connect LRU to be Integrated Load Software Test Drivers Run Test/Acquire and Analyze Data	Detailed Test Plan Detailed Test Procedures	Hardware Integration Test Report Updated Hardware Data Base	Hardware Test Equipment Software Test Drivers
2.41 Perform Stand Alone Module Tests	Review Test Procedure Set Up Test Run Test Acquire and Analyze Data	Coded/Debugged Module CPCI Module Detailed Test Plans/Procedures	Module Stand Alone Test Report Updated Software Data Base	Static Analyzer Dynamic Analyzer
2.42 Integrate Modules and Test Each CPCI	Review Test Procedure Set Up Test Run Test Acquire and Analyze Data	CPCI Module Integration Detailed Test Plan/Procedures Target Computer Verified Modules to be Integrated	Module Integration Test Report Updated Software Data Base	Software Test Drivers Program Library
2.43 Integrate System (Hardware & Software) in AISF	Integrate Subsystem LRU/Software Perform Test Analyze Results Correct Discrepancies Integrate Next LRU/Software and Repeat Above	Software Development Plan Hardware Integration Test Report Module Integration Test Report	System Integration Test Report Updated Hardware and Software Data Bases	AISF Hot Bench

*IEEE Standards 730-1981 and 829-1983.

TABLE 2.2-2. INTEGRATION PHASE ACTIVITIES & RELATED INTEGRITY ATTRIBUTED (Page 1 of 5)

Activity	Criteria	Parameters	Measures
2.1 Analyze Avionics Design Specifications	Service Life Reliability Maintainability Availability False Pulls (Retest OK) Cannot Duplicate (CND)	MTBF MTTR Time Limitations for Fault Isolation Maintenance Manhours/Flying Hours % False Pulls (Retest OK) % Cannot Duplicate	Degree of Completeness of Specification of each Parameter
2.2 Establish Avionics Integration Support Facility (AISF)	AISF Reliability AISF Maintainability AISF Availability	AISF System MTBF & MTTR AISF Subsystem MTBF & MTTR AISFV-Time Limitations Down-	Degree of Completeness of Requirements Skill Levels/No. of maintenance Personnel Test Equipment Complexity
2.3 Prepare AISF Program Plan	Budget Allocation Schedule	Man Hours/Activity Calendar Time/Activity Budget/Activity Milestones	Degree of Completeness of Description of each Activity & its Parameters
2.4 Prepare AISF Spec. (Type B1)	AISF Reliability AISF Maintainability AISF Availability	AISF System MTBF & MTTR AISF Subsystem MTBF & MTTR	Degree of Completeness of Specification of each Parameter
2.5 Allocate Functions to Man/ Hardware & Software	Workload Capability Utilized	Function(s) MTBF Function(s) Criticality % Minor Cycle Utilized % Major Cycle Utilized % Bus Capacity Utilized	Workload (Estimated)
2.6 Design AISF Architecture	AISF Functional Reliability AISF Functional Availability	Function(s) MTBF, MTTR	Degree of Completeness of (1) Design (2) Reliability Analysis (3) Maintainability Analysis (4) Capability Analysis
2.7 Establish Initial AISF Operating & Control Procedures	Performance Reliability Fail Active	Procedure-Time, Control Inputs, Process, Outputs	Degree of Completeness of Procedures
2.8 Prepare AISF Integration Plan	Schedule Resources Available Skills Available	Time Resources Required Skills Required	Degree of Completeness of: Integration Plan Steps in Plan
2.9 Prepare Hardware Development Specification (B2)	Service Life Reliability Maintainability Availability	Hardware MTBF Hardware MTTR Estimated Operating Time	Degree of Completeness of Specification of each Parameter

TABLE 2.2-2. INTEGRATION PHASE ACTIVITIES & RELATED INTEGRITY ATTRIBUTED (Page 2 of 5)

Activity	Criteria	Parameters	Measures
2.10 Procure Standard Hardware/Test Equipment	Capability of Equipment Reliability of Equipment Availability of Equipment	Accuracy Speed Memory Size Bandwidth MTBF MTTR	Degree of Conformance to Specification
2.11 Design New AISF Hardware	AISF Reliability AISF Maintainability AISF Capability	MTBF MTTR Accuracy Speed Bandwidth Memory Size Hardware	Failure Rates Clock Speed Clock Stability
2.12 Perform Hardware Preliminary Design Review	AISF Reliability AISF Maintainability AISF Capability	MTBF MTTR Accuracy Speed Bandwidth	Degree of Conformance of Design to Specifications
2.13 Perform Detailed AISF Hardware Design	AISF Reliability AISF Maintainability AISF Capability	MTBF MTTR Accuracy Speed Bandwidth	Failure Rates Clock Speed Clock Stability
2.14 Perform AISF Hardware Critical Design Review	AISF Reliability AISF Maintainability AISF Capability	MTBF MTTR Accuracy Speed Bandwidth	Degree of Conformance of Design to Specifications Degree of Conformance to Correcting PDR Discrepancies
2.15 Build AISF Hardware	AISF Reliability AISF Maintainability AISF Capability	MTBF MTTR Accuracy Speed Bandwidth Environmental Condition/Limits	Tests Passed Tests Failed Failures/Cause(s)
2.16 Integrate AISF Hardware	AISF Capability AISF Reliability	Man-Hours Computer Hours Test Equipment Hours MTBF	Time to Integrate Computer Time Used Failure(s)/Cause(s)
2.17 Prepare AISF Software Dev. Specs. (Type B5)	Software Architecture Module Complexity Module Size	Input Variables for Each Module Algorithms/Logic for Each Module Output Variables for Each Module	Degree of Completeness of Specification of Each Module

TABLE 2.2-2. INTEGRATION PHASE ACTIVITIES & RELATED INTEGRITY ATTRIBUTED (Page 3 of 5)

Activity	Criteria	Parameters	Measures
2.18 Procure Support Software	Cost Delivery Date	% Available % Validated	Degree of Conformance to Specification Degree of Completeness of Procurement Package
2.19 Design AISF Test Control, Test Drivers, Data Acquisition Software	Module Complexity Module Size	Number of Paths in Module Estimated Memory Requirements	Degree of Completeness of Software Design Description Report
2.20 Perform AISF Software PDR	Module Complexity Module Size	Number of Paths in Module Algorithm Complexity	Degree of Conformance to: (1) AISF Software Spec. (2) Software Design Description Report
2.21 Perform Detailed AISF Software Design	Software Reliability Module Complexity Module Size	Number of Modules Number of Paths in Each Module Algorithm Complexity/Accuracy	Degree of Completeness of (1) Detailed Design Description (2) Draft Software Product Specifications
2.22 Perform AISF Software CDR	Software Reliability Module Complexity Module Size	Number of Modules Number of Paths in Each Module Algorithm Complexity Accuracy	Degree of Conformance to: (1) AISF Software Dev. Spec. (2) Detailed Design Description
2.23 Code/Debug AISF Software	Software Reliability Memory Required	Number of Modules Number of Faults CPU Time	Software Faults Count Software Test Time Module's Paths Executed Lines of Code
2.24 Perform AISF Software Module Integration	AISF Software Reliability AISF Software Performance	Man-Hours Computer Hours Test Equipment Hours	Time to Integrate Time Used Failures/Cause(s)
2.25 Integrate AISF Software/ Hardware & Validate	AISF Reliability AISF Capability	Man-Hours Computer Hours Test Equipment Hours	Time to Integrate Set-up Time % Real-Time Resources Used
2.26 Complete Avionics Software Requirements Definition	Software Reliability Software Capability	Software Architecture Software Functions Software Module's Algorithms	Degree of Completeness of Requirements
2.27 Prepare Avionics CPCI Specifications	Software Architecture Module Complexity Module Size	Input Variables for Each Module Algorithms/Logic for Each Module Output Variables for Each Module	Degree of Completeness of Specification of Each Module
2.28 Commence Preliminary Design of Avionics Software	Module Complexity Module Size	Number of Paths in Module Estimated Memory Requirements	Degree of Completeness of Software Design Description Report
2.29 Perform Avionics Software PDR	Module Complexity Module Size	Number of Paths in Module Algorithm Complexity	Degree of Conformance to: (1) Software Specifications (2) Software Design Description Report

TABLE 2-2-2. INTEGRATION PHASE ACTIVITIES & RELATED INTEGRITY ATTRIBUTED (Page 4 of 5)

Activity	Criteria	Parameters	Measures
2.30 Perform Detailed Design of Avionics Software	Software Reliability Module Complexity Module Size	Number of Modules Number of Paths in Each Module Algorithm Complexity Algorithm Accuracy	Degree of Completeness of: (1) Detailed Design Description; (2) Software Design Description Report
2.31 Perform Avionics Software CDR	Software Reliability Module Complexity Module Size	Number of Modules Number of Paths in Each Module Algorithm Complexity Algorithm Accuracy	Degree of conformance to: (1) Software Dev. Spec.; (2) Detailed Design Description
2.32 Code/Debug Avionics Software	Software Reliability Memory Required	Number of Modules Number of Faults CPU Time	Software Faults Count Software Test Time Module's Paths Executed Lines of Code
2.33 Define Avionics Software Test Requirement	Software Metrics	Man-Hours AISF Host Computer Time Target Computer Time	Degree of Conformance to: Specification; Proven Test Methods
2.34 Develop CPCI Test Plans	Software Reliability	Number of Modules Number of Paths in Each Module Execution Time	Degree of Completeness of Test Plans & Procedures
2.35 Prepare Avionics System Integration Plan	System Reliability System Testability System Maintainability	MTBF Mean Fault Detection Time Test Thoroughness Mean Fault Isolation Time	Failure Rates Software Faults Count Degree of Completeness of Integration Plan & Procedures
2.36 Develop Detailed Test/Integration Plan for Each LRU	System Reliability System Testability System Maintainability	MTBF Mean Fault Detection Time Mean Fault Isolation Time Test Thoroughness	Degree of Completeness of Detailed Test Procedures of Each Step
2.37 Design/Build Cables	System Reliability System Maintainability	MTBF MTTR Man-Hours	Failures Rates Skill Level of Maintenance Personnel
2.38 Perform Incoming Test on Prototype LRUs	System Reliability	MTBF	Failure Rates Environmental Test Limits/values
2.39 Perform Stand Alone LRU Tests	System Reliability System Testability System Maintainability	MTBF Mean Fault Detection Time Mean Fault Isolation Time	Failure Rates Quantity of Faults Cause of Fault
2.40 Integrate/Test Hardware Systems' Subsystems	System Reliability System Maintainability System Testability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time MTTR	Failure Rates Quantity of Faults

TABLE 2.2-2. INTEGRATION PHASE ACTIVITIES & RELATED INTEGRITY ATTRIBUTED (Page 5 of 5)

	Activity	Criteria	Parameters	Measures
2.41	Perform Stand Alone Module Tests	Software Reliability Memory Used	Number of Modules Number of Faults CPU Time	Software Faults Count Software Test Time
2.42	Integrate Modules and Test Each CPCI	Software Reliability Memory Required	Number of Modules CPU Time	Software Faults Count Software Test Time
2.43	Integrate System (Hardware & Software) in AISF	System Reliability System Testability System Maintainability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time MTTR	Failure Rates Software Faults Count Software Test Time
2.44	Test System Integration in AISF	System Reliability System Testability System Maintainability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time MTTR	Failure Rates Software Faults Count Software Test Time
2.45	Integrate System Into Aircraft	System Reliability System Testability System Maintainability	MTBF Mean Fault Detection Time Mean Fault Isolation Time	Failure Rates Software Faults Count Software Test Time System Test Time
2.46	Develop System Validation Test Plan & Procedures	System Reliability System Testability System Maintainability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time MTTR	Degree of Completeness of Validation Test Plan and Procedures
2.47	Perform System Validation Tests	System Reliability System Testability System Maintainability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time MTTR	Failure Rates Software Faults Count Software Test Time System Time
2.48	Perform Flight Tests	System Reliability System Testability System Maintainability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time MTTR	Failure Rates Software Faults Count Software Test Time System Time
2.49	Perform OT&E	System Reliability System Testability System Maintainability System Availability	MTBF Mean Fault Detection Time Mean Fault Isolation Time	Failure Rates Software Faults Count System Time
2.50	Production & Deployment			
2.51	Operation & Maintenance	System Supportability		

requirements of the facilities in terms of the space required, electrical power required, and environmental conditions in the facility as well as environmental test requirements which must be provided by the facility. The analysis must necessarily concern itself with the human resources required to develop and operate the facility. Time which is treated as a resource, as well as the skill levels of personnel, should be determined during the analysis.

The analysis should determine the specific types of tests required for integration of the avionics, items required to conduct the test, and the requirements for data acquisition and reduction.

When possible, the analysis should determine the availability of the resources as well as those which must be designed and developed in order to provide the capability required from the AISF.

The Avionics Integration Support Facility (AISF) should be contracted for "up front" as a deliverable under the scope of the contract. The AISF should be developed and used by the integrating contractor up to the point of field deployment; at which time it should then be delivered to the government logistics/maintenance organization that will have full responsibility for the system.

Without this facility the government does not have the capability to dynamically test the individual components (subsystems or systems) in a "near-real" environment using other "real" equipments, cables, etc. which normally interface with the unit under test.

The output of this task is an AISF requirements document and an AISF data base which reflects the requirements determined from the analysis.

Table 2.2-2 presents the integrity measures, parameters, and criteria for this activity.

2.2.3 Prepare AISF Program Plan (Activity 2.3)

The AISF Program Plan is developed using the previously defined AISF requirements. This plan organizes all tasks required to develop the AISF in the form of a work breakdown structure. Included for each item in the work breakdown structure is an associated statement of work, schedule, resources required, and budget. The responsible group or manager for each item in the work breakdown structure is included in the program plan.

The program plan also includes a description of the procedures which will be used to control the work during subsequent phases of the system life cycle. It includes definition of both technical and financial management tools and describes the reporting procedures in detail. The program management methods such as project control tools, required back-up staff, and line-management structure are defined.

The output of this task is the AISF program plan.

Table 2.2-2 presents the integrity and information associated with this activity.

2.2.4 Prepare AISF Specification (Type B1) (Activity 2A)

The prime item development specification for the avionics integration support facility will incorporate (directly or by reference) the AISF requirements contained in the requirements document. Specifications shall identify all of the major components of the AISF and the individual components which must be developed.

The characteristics in the AISF data base related to performance, physical characteristics, reliability, maintainability, and environmental conditions shall be included in the specification.

The specification shall be developed in the format prescribed for a Type B1 as given in MIL-STD-490.

This specification can be typed on a word processor which will permit its subsequent use in developing the corresponding products specification.

Integrity attributes related to this activity are contained in Table 2.2-2.

2.2.5 Allocate Facility Functions to Man/Machine Hardware and Software (Activity 2.5)

Prior to initiating this activity, the overall AISF design may be indirectly improved until a preferred design concept satisfies the performance, reliability, maintainability, and safety goals as defined in the specification. This activity assumes that the basic concepts meets these requirements.

There is no cut and dried procedure for allocation of the functions to the operators of the facility as opposed to the hardware and software of the facility.

Typically, the operators of the facility will perform the physical connections for each test to be run. Software and hardware collectively may, under operator control, run the tests, acquire the data, and then develop and present results of the analysis. The operator must interpret these results.

The inputs to this activity are the AISF requirements document, the AISF data in the data base, and the AISF specificatior. The output is the AISF Function Allocation Report.

Integrity attributes to this activity are listed in Table 2.2-2.

2.2.6 Design AISF Architecture (Activity 2.6)

The architecture of the AISF must provide capabilities for multi-user operation since many system integration steps occur in parallel. This necessitates having the capability to permit addition of the next LRU when the system is being integrated on the hot bench while other personnel are performing stand-alone tests on software or hardware.

The architecture must not only have a great deal of flexibility, but also contain sufficient redundancy in computers and data paths to permit continued operation of the facility in the case of failure or scheduled maintenance on a hardware subsystem in the facility.

The principal human interfaces with the avionics integration support facility are the test control centers which integrate the facility computers' input/output ports, general test equipment, data acquisition and display devices, and avionics and facility power distribution and control. The test control centers are interconnected to the facility processors through computer data buses.

Facility stand-alone test stations, microprocessor development systems, the hot bench, and fixed base fuselage stations containing cockpit controls and displays are interconnected through the test control centers to the facility processors.

The architecture of the facility should be developed based upon the overall facility's required availability and capability. Consideration should be given to the need for both scheduled maintenance and unscheduled maintenance.

The input to this activity is the AISF Function Allocation Report, the AISF specification, the AISF data and the data base and the AISF requirements document. The output is the AISF Architecture Report.

Integrity attributes for this activity are given in Table 2.2-2.

2.2.7 Establish Initial AISF Operating and
Control Procedures (Activity 2.7)

The AISF operating and control procedures involve those procedures associated with the operation and use of the AISF hardware and software in conjunction with the avionics system which will be integrated using the facility. These operating and control procedures are based upon the previously performed allocation of functions to the facility operators (man) and the hardware and software. The procedures shall be designed to minimize human error impacting the operation and use of the facility. This will require development of procedures to provide a friendly user interface to the personnel using the facility. Human interaction with the computer software should make use of modern software tools including "Help" features in such a manner that the time required to train personnel to use the facility will be minimized.

The inputs to this activity include the AISF architecture report, AISF requirements document, AISF specification, AISF function allocation report, and the AISF data in the data base. In addition, data on existing facilities' operating and control procedures shall be considered. The output will be the preliminary system operating control procedures report.

Integrity attributes for this activity are given in Table 2.2-2.

2.2.8 Prepare AISF Integration Plan (Activity 2.8)

The AISF integration plan is developed based upon information contained in the schedules for each of the hardware and software items in the work breakdown structure in the AISF program plan as well as the AISF architecture. Using this information and that contained in the specification and the data base, an integration plan including the sequence of integration steps and the procedures to be followed shall be developed. The output of this activity is the AISF integrated plan.

Integrity attributes for this activity are contained in Table 2.2-2.

2.2.9 Prepare Hardware Development Specification (B2) (Activity 2.9)

Specifications shall be prepared for all hardware to be used in the AISF. This includes standard hardware which can be procured "off the shelf", including test equipment, as well as new hardware which must be designed in order to provide the interfaces not available off-the-shelf.

Primary inputs to the preparation of the hardware specifications are the AISF specification, system software interface specification, hardware ICD's, LRU specifications, and the system specifications. The outputs are the individual hardware specifications for both hardware to be procured from off-the-shelf as well as hardware to be designed.

Table 2.2-2 contains the integrity attributes for this activity.

2.2.10 Procure Standard Hardware/Test Equipment (Activity 2.10)

This activity requires developing the procurement packages based upon each of the standard hardware items specification previously prepared. A procurement package must be prepared for each hardware item. After issuing the RFQ and receiving the bids, contracts are ordered for the hardware and test equipment.

The integrity atrributes for this activity are contained in Table 2.2-2.

2.2.11 Design New AISF Hardware (Activity 2.11)

The inputs to this activity are the development specifications for the new hardware. Procurement packages must be prepared, RFPs issued, bids evaluated, and contract awarded to develop new hardware items.

The selected contractors shall then design the new hardware required for the AISF. A contractor may elect to use manual design practices or may use computer aided design (CAD) practices. In either case, part selection, screening, control, and assembly will be required. If a data base system is used, characteristics of the qualified parts may be contained in that data base. Otherwise, the contractor must use manual look-up techniques to perform part selection.

The integrity attributes relative to this activity are given in Table 2.2-2.

2.2.12 Perform AISF Hardware Preliminary
Design Review (PDR) (Activity 2.12)

The inputs to the hardware preliminary design review are the individual hardware design description documents, and hardware development specifications. The purpose of the design review is to review areas such as hardware trade-offs, functional interfaces, errors due to lack of understanding of the critical design areas, and the interfaces of the system's integration/support facility with each of the hardware items. Results of the preliminary hardware design review are discrepancy reports which document the agreed to corrective actions.

The integrity attributes for this activity are contained in Table 2.2-2.

2.2.13 Perform Detailed AISF Hardware Design (Activity 2.13)

The inputs to this activity are the discrepancy reports from the hardware preliminary design review. After completion of the preliminary design review, the manufacturer should update all specifications and drawings to reflect any changes resulting from the design review action items. The updated specifications and drawings are then used in the detailed design.

The manufacturer performs the detailed design of the hardware comprising each of the subsystems. This is likely to require breadboarding and evaluation of any new circuits. In addition to the performance evaluation, the manufacturer may acquire samples of the selected parts and subject these samples to parts screening. Parts screening methods shall be identical to those previously described in the design section of this report, with screening performed at environmental levels contained in the specification.

Those parts which survive the screening should be placed under parts control.

The output of this activity would consist of recommended changes to the baseline design established at the hardware preliminary design review, documented as updates to specifications and drawing.

Table 2.2-2 contains the integrity attributes for this activity.

2.2.14 Perform AISF Hardware Critical Design Review (Activity 2.14)

The inputs to the hardware critical design review are recommended updates to the preliminary design baseline based upon the design evaluation and performance tests. These recommended changes are considered by the reviewers and either approved or noted as an action item requiring resolution. Once these action items are resolved, the specifications are updated to reflect the design baseline which will be used by configuration management in the subsequent phases.

The output of this activity are these updated specifications and the drawings which will be used to build the AISF hardware.

The integrity attributes for this activity are contained in Table 2.2-2.

2.2.15 Build AISF Hardware (Activity 2.15)

The inputs to this activity are the specifications and the drawings of the hardware to be built. Parts assembly will be made using mainly manual assembly processes since the volume for automatic assembly is usually not warranted for one of a kind items.

After assembly of the parts, parts shall be subjected to inspection followed by qualification level testing. The individual cards in the case of electronics shall then be assembled into the completed hardware items. Testing will be conducted to the levels contained in the hardware development specification.

The output of this activity is the AISF hardware which will be integrated with the standard "off the shelf" hardware in the integration activity.

The integrity measures for this activity are given in Table 2.2-2.

2.16 Integrate AISF Hardware (Activity 2.16)

This activity involves a step-by-step integration of the AISF hardware according to the AISF integration plan. Each hardware item shall, whenever practical, have been subjected to a stand-alone test prior to integration with another hardware item. This includes both the standard hardware as well as the new hardware designed for the AISF. The build-up of an AISF or the modification of an existing AISF to integrate new system components must be

done methodically and the results of each integration step carefully documented.

Prior to the actual physical integration of the AISF hardware, the facility in which the AISF hardware will be installed must meet the requirements of the AISF specification. Particular attention must be paid to the AISF power distribution system and grounding.

An extensive list for the inputs required to perform this activity can be found in many AISF integration plans. Table 2.2-1 presents only some of the high level inputs. Additional detail can be found in the AISF references.*

The output of the activity is the fully checked out AISF hardware.

Table 2.2-2 contains integrity attributes related to this tsk.

2.2.17 Prepare AISF Software Development Specifications (Type B5) (Activity 2.17)

This top level AISF Software Development Specification implements the requirements for the functions allocated to the AISF software and the AISF operating control procedures required to efficiently utilize the AISF. This specification includes the compilers, assemblers, linkers, editors, and loaders (for the flight processors) which will be resident on the support facility host processors. The specification also includes support software required for the development, test, and integration of the object code for each processor is in the avionic system. In addition, the specification includes all simulation software, test driver software, and data acquisition software required to implement the AISF software functions.

The high level inputs for this activity as well as the output tools are given in Table 2.2-1. Note that it is not a single AISF software development specification but rather a development specification for each of the major software categories previously mentioned.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.18 Procure Support Software (Activity 2.18)

Software such as compilers, assemblers, linkers, editors, and loaders (for the flight processor) which are not available are typically pro-

---

* Hanson, Jon G., "Design and Implementation of USAF Avionics Integration Support Facilities", AFIT/GCS/EE/81D-10, Air Force Institute of Technology, 1982. Angrist, Elsa F., "A Survey of Avionics Simulation Facilities", MV-409-012-TAC/AFOAA, Federal Computer Performance Evaluation Center, August 1974.

cured from the computer manufacturers or independent software agents if not furnished as government furnished software. This activity involves procurement of this software using as input the software development specifications for those items which are to be procured. Table 2.2-1 lists some major subactivities for this activity as well as the tools used in preparing the procurement package and contract.

Table 2.2-2 lists the integrity attributes associated with this activity.

2.2.19 Design AISF Test Control, Test Drivers, Data Acqusition Software (Activity 2.19)

Normally the avionic systems integrator designs and develops the avionics integration support facility software that is not procured.

The objective of this activity is to develop the initial design documents for each of the individual software programs, modules, or routines. The individual software design documents are the basis for the preliminary design review for that component of the software. Using a structured design procedure, each module is designed using the allowed basic constructs and the algorithms defined in the development specifications.

The software documents must identify each module, the module's data flow, associated structure diagram, and the associated data tables.

Whenever possible, modern software engineering tools (HITT82)* should be used rather than manual methods since these tools provide consistency and tend to eliminate the variability due to human error in the design process.

The output of this activity is the software design description report for each of the major software categories.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.20 Perform AISF Software Preliminary Design Review (Activity 2.20)

The Preliminary Design Review is a formal technical review of the basic design approach for the AISF software. There may be a PDR for each software package used on a particular AISF computer. A collective PDR may be held for functionally related groups of programs.

---

* Hitt, Ellis F., Webb, Jeff, Lucius, Charles, Bridgman, Michael S., and Eldredge, Donald, "Handbook -- Volume 1, Validation of Digital Systems in Avionics and Flight Control Applications," DOT/FAA/CT-82/115, Battelle Columbus Laboratories, December 1982.

The responsibility for conducting the PDR rests with the organization responsible for the design activity. During the review, the reviewers are expected to comment on the completeness, accuracy, and general quality of the work. At the completion of the design review a summary report is issued noting discrepancies between the software development specifications and the design and the modules requiring further design or redesign prior to the critical design review.

Table 2.2-2 lists the integrity attributes associated with this activity.

2.2.21 Perform Detailed AISF Software Design (Activity 2.21)

The inputs to this activity are the inputs and outputs of the previous activity, 2.20. The final software design is often done using a formal design methodology such as structured design or other methods. During the final design effort, a design walk-through should be used by the developers to verify the flow and logical structure of the software while design inspections should be performed by the test team.

Table 2.2-1 summarizes the sub-activities, inputs, and outputs of this activity.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.22 Perform AISF Software Critical Design Review (CDR) (Activity 2.22)

The Critical Design Review is a formal technical review of the detailed design conducted prior to the start of coding. CDR is intended to insure that the detailed design satisfies the performance requirements of the development specifications. A Critical Design Review is also accomplished for the purpose of establishing integrity of computer program design at the level of flow charts, and computer program logical design prior to coding and testing. The principal items reviewed are the complete draft of the AISF product specifications and the drafts of the test plans/procedures. All changes to the development specifications and available test documentation are examined to determine compatibility with the test requirements of the development specification.

After resolution of any action items resulting from the design review, the resultant design is released to configuration control and becomes a software design baseline.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.23 Code/Debug AISF Software
(Activity 2.23)

This activity involves the actual coding in the selected language and debugging of the code. Code walk-through and code inspection are manual techniques for verification of the code. Assembling or compiling the code also provides a debug for those errors the compiler or assembler is designed to detect. Errors found during the debug should be corrected before beginning coding of another module.

Table 2.2-1 summarizes the inputs, outputs, and tools used in this activity.

Table 2.2-2 lists the integrity attributes associated with this activity.

2.2.24 Perform AISF Software Module Integration
(Activity 2.24)

The AISF Software Modules shall be integrated using the approach specified in the AISF integration plan. The integration testing is primarily functional with the main emphasis on the interaction between the software components and the interfaces. As each test is conducted, a test report shall be generated. After all testing is completed for the code resident on a support facility computer, the final test report should be prepared which includes all errors detected and status of their correction. The AISF software data base also should be updated to reflect that information.

Table 2.2-1 summarizes the inputs, outputs, and tools used in this activity. Integrity attributes associated with this activity are listed in Table 2.2-2.

2.2.25 Integrate AISF Software/Hardware and Validate
(Activity 2.25)

This activity consists of integration of the AISF system software and hardware and the final validation of the AISF. The software and hardware integration sequence will follow that in the AISF integration plan. As each step is completed, discrepancies shall be noted and corrected prior to proceeding to the next step in the integration and validation sequence. The results of each test will be documented and the AISF software data base updated.

Table 2.2-1 summarizes the inputs and outputs of this activity.

Integrity attributes for this activity are given in Table 2.2-2.

2.2.26 Complete Avionics Software Requirements Definition
(Activity 2.26)

The system integrator will completely define all software functions, and initial system operating and control procedures. The software architecture will be defined. The software functions to be performed by each process are defined in terms of their control structure, data structure, data flow control, and application structures.

The operating system functions of request handling/interrupt control, task control (scheduling and dispatching), resource allocation, and fault monitoring should be described. The data base, data flow control in a distributed system, and the application modules which implement the system functions should be described. The application's functional description should include the input, algorithms to be used, accuracy, constraints, and output.

The system software development specification will describe the overall system software requirements.   This specification will be the primary reference document for all systems software. Software located in individual processors will be traceable back to this system software development specification.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.27 Prepare Avionics Computer Program Configuration Item
(CPCI) Specifications (Activity 2.27)

The objective of this set of activities is to develop detailed computer program configuration item (CPCI) specifications. These specifications are a statement of the development requirements for each CPCI, whether they are subroutines, programs, groups of programs, or the entire software subsystem. The individual CPCI specification shall be traceable to the software development plan, configuration item index, and system software development specification.

The integrity attributes for this activity are given in Table 2.2-2.

2.2.28 Commence Preliminary Design of Avionics Software
(Activity 2.28)

Figure 2.2-2 indicates the relationship of this activity to other software activities in the system cycle. The input to the preliminary design prccess is the system software interface specification the computer program configuration item (CPCI) development specifications, and the software development plan.

The individual software design documents should be developed using the structured design procedure. Each module should be designed using the allowed basic constructs and the algorithm defined in the CPCI development
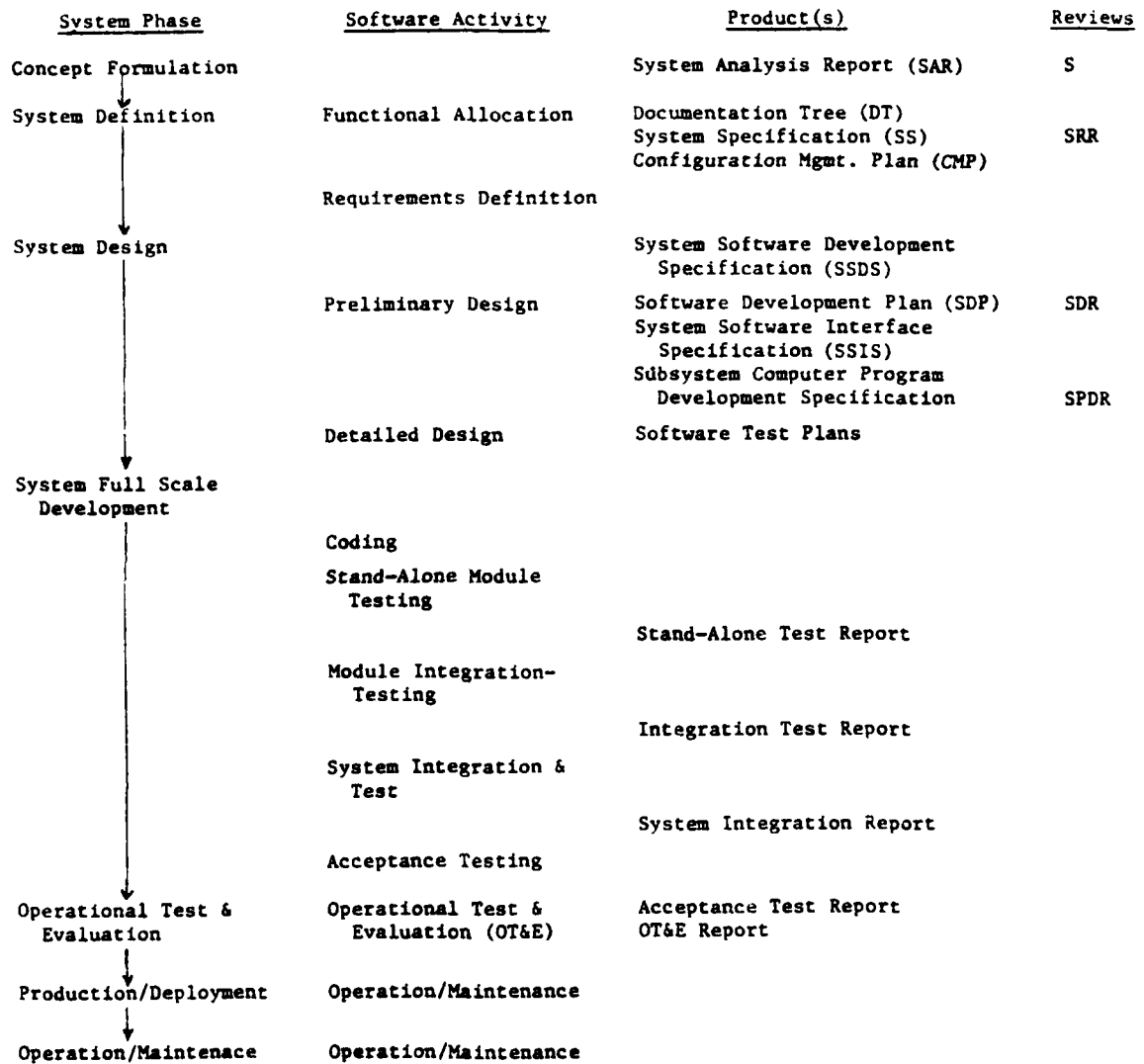
System Phase	Software Activity	Product(s)	Reviews
Concept Formulation		System Analysis Report (SAR)	S
System Definition	Functional Allocation	Documentation Tree (DT)	
		System Specification (SS)	SRR
		Configuration Mgmt. Plan (CMP)	
	Requirements Definition		
System Design		System Software Development Specification (SSDS)	
	Preliminary Design	Software Development Plan (SDP)	SDR
		System Software Interface Specification (SSIS)	
		Subsystem Computer Program Development Specification	SPDR
	Detailed Design	Software Test Plans	
System Full Scale Development			
	Coding		
	Stand-Alone Module Testing		
		Stand-Alone Test Report	
	Module Integration-Testing		
		Integration Test Report	
	System Integration & Test		
		System Integration Report	
	Acceptance Testing		
Operational Test & Evaluation	Operational Test & Evaluation (OT&E)	Acceptance Test Report OT&E Report	
Production/Deployment	Operation/Maintenance		
Operation/Maintenace	Operation/Maintenance		

FIGURE 2.2-2. Software Activities/Products Relation to System Life Cycle Phases

specification. The CPCI design documents identify each module, the module's data flow, associated structure diagram, and the associated data tables.

In performing the design, it is important that the design team not "reinvent the wheel". Design is typically an intellectual process based upon the knowledge of the designer. The designer should, whenever practical, use standard software modules which have been utilized previously in USAF aircraft (HITT81).*

Table 2.2-1 summarizes the input, output, and tools associated with this activity.

The integrity attributes for this activity are given in Table 2.2-2.

2.2.29 Perform Avionics Software Preliminary Design Review (PDR) Activity 2.29)

The Preliminary Design Review is held prior to the start of the detail design. The design review team is concerned with determining the consistency of the preliminary design with the requirements, the adequacy of the test requirements, and the software development and support tools planned for use during program development.

Prior to the design review, the design team will often have performed an inspection of the code. During the formal preliminary design review, the designer may present a brief overview and then walk the reviewer through the design in a step-by-step fashion that simulates the function under investigation. The materials should be reviewed in enough detail so the concerns expressed at the beginning are either explained away or identified as action items. Significant factors that require further action are recorded as they are identified. These action items are included in the software preliminary design review report. This is the output of this activity.

After resolution of the action items, the resultant design is released into the control cycle according to the prescribed configuration control methods.

Table 2.2-1 summarizes the subactivities, documentation, and tools used during preliminary design review.

The integrity attributes for this activity are given in Table 2.2-2.

---

* Hitt, Ellis F. and Broderson, Robert L., "Integrated Control Core Software Concept Study", AFWAL-TR-81-3141, Battelle Columbus Laboratories, December, 1981.

2.2.30 Perform Detailed Design of Avionics Software
(Activity 2.30)

The detailed design of the software is often done using the same concept that the preliminary design utilized. This is normally a formal design methodology based upon some structured design practices. During the final design effort, the design walk-through should be used by the developers to verify the flow and logical structure of this system. Design inspection should be performed by the test team. The output of the detailed design phase is the detailed design document which is the basis for the critical design review.

Table 2.2-1 summarizes the subactivities, inputs, and outputs for this activity.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.31 Perform Avionics Software Critical
Design Review (CDR) (Activity 2.31)

The critical design review is a form of technical review of the CPCI detailed design and is conducted prior to the start of coding. CDR is intended to insure that the detailed design solutions, as reflected in the draft of a CPCI product specification satisfy performance requirements established by the CPCI development specification. The CDR is also accomplished for the purpose of establishing integrity of the computer program design at the level of flow charts or program design language syntax prior to coding and testing. The principal items reviewed are the complete draft of each CPCI product specification and drafts of test plans/procedures. All changes to the CPCI development specification and available test documentation are examined to determine compatibility with the test requirements of the development specification. After resolution of any action item resulting from the design review, the resultant design is released to configuration control and becomes a software design baseline.

Table 2.2-1 summarizes the subactivities, inputs, and outputs for this activity.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.32 Code/Debug Avionics Software (Activity 2.32)

If a program design language such as Ada* was used in the design, it is possible that the program design language (PDL) was compiled. The designers may have elected to use the PDL with a separate PDL processor; if

---

* Ada is a trademark of the U.S. Department of Defense (Ada Joint Program Office).

this was the case, a separate effort to implement the design in compatible Ada is required. Errors found during the compilation should be corrected before beginning coding for another module.

Table 2.2-1 lists the subactivities, inputs, and outputs associated with this coding and debugging activity.

The integrity attributes for this activity are given in Table 2.2-2.

2.2.33 Define Avionics Software Test Requirements (Activity 2.33)

The test requirements document describes the software test approach and addresses:

(1) The software testing philosophy to be followed.

(2) Responsibility for the various levels of testing.

(3) Software performance measures and standards.

(4) Method to be following and handling software change proposals originating from the test group.

(5) Test report requirements.

The output of this activity is the test requirements document which is used for the detailed test planning, development of test procedures for each test plan.

Table 2.2-2 presents the integrity attributes related to this activity.

2.2.34 Develop CPCI Test Plans (Activity 2.34)

These test plans will be developed for each of the test levels including: (1) stand-alone testing of modules; (2) software module integration; (3) system hardware and software integration; and (4) flight test.

Each test plan shall specify the methodology to be employed (see Figure 2.2-3). The test plan shall trace the testing sequence from unit level testing to final acceptance testing and identify each individual test. Test procedures keyed to the test plan provide step-by-step instructions for the execution of the test and specify precisely what outputs are to be expected.

Test support software for the hardware test bed to be used should be identified as well as all testing inputs.

The test procedures shall be sufficiently detailed that they can be used in the complete integration, replication, and validation of the system

1. INTRODUCTION

    1.1 SCOPE
    1.2 APPLICABLE DOCUMENTS
    1.3 PURPOSE
    1.4 SYSTEM OVERVIEW

2. SOFTWARE TEST MANAGEMENT

    2.1 GENERAL SOFTWARE TEST OBJECTIVES
    2.2 SOFTWARE DEVELOPMENT PLAN (SCHEDULE OF ALL SOFTWARE ACTIVITIES)
    2.3 DOCUMENTATION/STORAGE OF TESTS

3. VERIFY SYSTEM SOFTWARE DEVELOPMENT SPECIFICATION AGAINST SYSTEM
   REQUIREMENTS

    3.1 PROCEDURES
    3.2 DESIGN REVIEW
    3.3 REPORT RESULTS

4. VERIFY SUBSYSTEM COMPUTER PROGRAM CONFIGURATION ITEM DEVELOPMENT
   SPECIFICATION AGAINST SYSTEM SOFTWARE DEVELOPMENT SPECIFICATION

    4.1 PROCEDURES
    4.2 DESIGN REVIEW
    4.3 REPORT RESULTS

5. TEST MODULES

    5.1 GENERAL TEST CRITERIA
    5.2 GENERAL TEST PROCEDURE
    5.3 BY MODULE

        5.3.1 SPECIFIC TESTS
        5.3.2 TEST TOOLS

6. VERIFY CODE OF SUBSYSTEM COMPUTER PROGRAM CONFIGURATION ITEM DEVELOPMENT
   SPECIFICATIONS

    6.1 PROCEDURES
    6.2 DESIGN REVIEW
    6.3 REPORT RESULTS

FIGURE 2.2-3. System and Subsystem Software Test Plans

7. TEST MODULE INTEGRATION

    7.1 GENERAL TEST CRITERIA
    7.2 SOFTWARE DEVELOPMENT PLAN (HIERARCHICAL BLOCK DIAGRAM OF MODULE
         INTERCONNECTIONS)
    7.3 GENERAL TEST PROCEDURE (INTEGRATION PLAN)
    7.4 BY GROUP

         7.4.1 SPECIFIC TESTS
         7.4.2 TOOLS

8. SYSTEM TESTING

    8.1 GENERAL TEST CRITERIA
    8.2 SYSTEM REQUIREMENTS VERSUS TEST MATRIX
    8.3 SYSTEM VERIFICATION

         8.3.1 DEFINITION
         8.3.2 SIMULATION

                8.3.2.1 ENGINEERING MODEL
                8.3.2.2 PROTOTYPE

         8.3.3 HOT BENCH (TEST HARDWARE/SOFTWARE INTEGRATION)

                8.3.3.1 PRODUCTION PROTOTYPE

    8.4 SYSTEM VALIDATION

         8.4.1 DEFINITION
         8.4.2 IRON BIRD
         8.4.3 FLIGHT TEST

9. SOFTWARE MAINTENANCE/REGRESSION TESTING

    9.1 GENERAL TEST CRITERIA
    9.2 GENERAL TEST PROCEDURE
    9.3 BY MODULE AND GROUP REQUIRING RETEST

         9.3.1 SPECIFIC TESTS

              FIGURE 2.2-3. System and Subsystem Software Test Plans
                                    (Continued)

software. The test procedures must provide all information required for integration of the system and flight test of the system.

The method to be followed in updating the software data base and the documentation of test results shall be included in the test plan.

Table 2.2-2 contains the integrity attributes for this activity.

2.2.35 Prepare Avionics System Integration Plan (Activity 2.35)

The avionics systems integration plan shall document the process to be followed in the integration of the avionics system. This shall include the sequence of steps to be followed in the integration, the sequence of tests within each integration step, the equipment required to complete each integration step, and the hardware and software to be integrated. In addition, the test hardware and test driver software to be used in the integration shall be specified.

The integration test plan shall also contain a complete definition of cables, connectors, and interfaces required to complete the integration test within a step.

The integration plan shall also specify the data to be acquired and the reduction procedures to be used in the analysis of those data for each integration step.

Table 2.2-2 contains the integrity attributes related to this activity.

2.2.36 Develop Detailed Test/Integration Plan
for Each Test LRU (Activity 2.36)

This activity involves developing a test plan for each sequence of steps for each step in the integration sequence of the LRUs. It also involves developing detailed test procedures for each step. Table 2.2-3 provides an outline of the typical test plan content and Table 2.2-4 provides an outline of the detailed test procedure.

These test plans and test procedures can be developed manually or a word processing system can be used to ? the outline of the sample test plan and sample test procedure with the user merely filling in the appropriate paragraph or blanks for the specific test procedure.

Table 2.2-1 summarizes the inputs and outputs for this activity.

The integrity attributes for this activity are given in Table 2.2-2.

2.2.37 Design/Build Cables (Activity 2.37)

This activity involves designing, acquiring the parts, and building the cables required not only to integrate the avionics LRUs but also to integrate the LRUs with the AISF hardware.

Table 2.2-1 summarizes the subactivities, inputs, outputs, and tools used for this activity.

The integrity attributes for this activity are contained in Table 2.2-2.

2.2.38 Perform Incoming Tests on Prototype LRUs (Activity 2.38)

Incoming prototype LRUs shall be subjected to incoming inspection plus acceptance testing if not conducted at the manufacturer's facility.

Table 2.2-1 summarizes the subactivities, inputs, outputs, and tools for this activity.

Table 2.2-2 lists the integrity attributes for this activity.

2.2.39 Perform Stand-Alone Test on LRUs (Activity 2.39)

The prototype hardware subsystem LRUs shall be subjected to stand-alone tests. This test shall be performed using the configuration, hardware and software required for the test, stand-alone test sequence, and functional test check list prepared for each LRU in activity 2.36.

In addition, failure modes and effect tests should be conducted at the individual subsystem level to verify those failure modes predicted for an LRU. After undergoing the initial peformance test, the LRUs shall be subjected to environmental qualification testing at the level contained in the test plan.

Any discrepancies identified in the test should be analyzed and modifications required to make the system operate properly identified and submitted to the change control board.

Table 2.2-1 summarizes the subactivities, inputs, and outputs for this activity.

The integrity attributes associated with this activity are contained in Table 2.2-2.

2.2.40 Integrate/Test Hardware Systems' Subsystems (Activity 2.40)

This activity consists of a sequence of integration tests to integrate each of the hardware subsystems. The sequence of integration tests is defined in the detailed test/integration plan for each LRU.

The test plan must identify the test objectives, test configuration, hardware and software required, the integration sequence and responsibilities, and provide a functional check list which contains all functions to be performed and the values to be verified.

A simulator may be used in this testing to provide the test driver signal for items not yet integrated.

The output of each integration step in the sequence is a test report which documents any discrepancies or anomalies noted as well as those test procedures which were successfully completed. Those items which are to be corrected will, after correction, be retested following the same test procedure for that step which had failed.

Table 2.2-2 contains the integrity attributes for this activity.

2.2.41 Perform Stand-Alone Module Test (Activity 2.41)

The stand-alone module test may use the techniques of:

(1) Static analysis,
(2) Dynamic testing with or without instrumentation probes,
(3) Symbolic execution, and
(4) Proofs of correctness.

Code execution testing may be done on a host computer which simulates or emulates the target computer or the actual execution may be done on the target machine.

Whichever module testing approach is taken, one basic criterion for the set of test cases is to insure that every instruction in the module is executed at least once. All logical paths should also be traversed. The testing should be done in the sequence specified by the test plan and procedure. The result of the stand-alone test should be documented in a stand-alone test report noting any discrepancies that will necessitate retesting.

The integrity attributes associated with this activity are given in Table 2.2-2.

2.2.42 Integrate Modules and Test Each CICI (Activity 2.42)

The software developer shall integrate modules using the method specified in the test plan and test procedures.

Integration testing is primarily functional with the main emphasis on the interaction between the software components and their interfaces. Testing shall take place in the laboratory containing the target computers and enough equipment to simulate the application with considerable fidelity. As

TABLE 2.2-3. TEST PLAN CONTENTS

A test plan is to be written for each set of tests to be performed during the development and integration. The general contents of each test plan should be as follows:

1. Test Objectives
    (This should be a concise description of the objective of the test including the criteria to be used to determine if the item under test fully satisfied the test objectives, partially satisfied the test objectives, or failed the test.)

2. Functional Test Requirements
    (This section should describe the test configuration, including hardware interconnection cabling, and support hardware, and software.)

3. Test Requirements
    (A complete description of the electrical, physical, and software inputs for each of the preliminary and functional tests shall be given. The expected outputs from the item under test for each of the inputs shall be described. The data to be collected shall be identified.)

4. Data Acquisition
    (This section shall describe the method to be used to acquire and record input and output data to be used in the test's analysis and evaluation step.)

5. Data Reduction, Analysis, Test Evaluation
    (This section should completely describe the data reduction and analysis procedures. This section should also contain the description of the method to be used to evaluate the results of the tests based upon the results of the data analysis.)

6. Test Procedures
    (This should be a complete description of each of the steps the technicians and engineers take in performing the test including the test setup, preliminary test, and functional test. After completing these procedures, the data should be available for reduction and subsequent analysis. These procedures can be included in an appendix by reference from the main paragraph in the body of the test plan.)

7. Responsibilities and Support Requirements
    (This section should define the support requirements and responsibilities.)

TABLE 2.2-4. DETAILED TEST PROCEDURE
(Outline)

TITLE: _____   Sequence No:
                                       Responsible Engineer:

A. TEST OBJECTIVES
    (Set of statements defining purpose of the integration sequence and/or
    tests in terms of the general objectives.)

B. TEST DESCRIPTION
    (A brief description of the integration sequence and/or test, mission
    scenario, and basic test experiment approach.)

C. TEST CONFIGURATION
    (Block diagram depicting all hardware interconnections with connectors and
    cabling lists.)

D. MISSION SOFTWARE CONFIGURATION
    (Statement of mission software configuration to be loaded and method of
    loading.)

E. PRE-TEST REQUIREMENTS
    (Statement as to the conditions and other integration or test sequences
    which must be satisfied prior to the implementation of their integration
    sequence or test.)

F. TEST SUPPORT HARDWARE
    (A list of the test support hardware by item and serial number.)

G. TEST SUPPORT SOFTWARE
    (A list of simulation software programs and data files required for this
    test.)

H. FACILITY REQUIREMENTS
    (Statement of the space, power, and cooling facilities requirements for
    the tests.)

I. RESOURCE REQUIREMENTS
    (Statement of personnel - test engineers, technicians, contract engineers,
    etc. - to perform the integration and testing.)

J. DATA ACQUISITION
    (Measurements list, format, scaling, recorder channel assignment, recorder
    speeds, sampling rates and events, and test forms.)

TABLE 2.2-4. (Continued)

K. OPERATING PROCEDURES
    (Step-by-step sequence of operator instructions for integration and test
    including:
    a. Test Set Up
    b. Test Operation
    c. Data Acquisition
    d. Acceptance/Failure Criteria for Test.)

L. CHECKLIST (Test Record)
    (Step-by-step checklist for recording the results of each step-by-step
    procedure.)

M. DATA REDUCTION PROCEDURES
    (List of programs and procedures to be used in reducing, editing, and
    analyzing data.)

N. POST TEST REQUIREMENTS
    (Statement as to any restriction imposed on subsequent tests.)

O. SUPPORT DOCUMENTATION REFERENCES
    (A list of supporting documentation.)

each test is conducted, a test report shall be generated. After all testing is completed the final report is generally prepared which includes all errors detected and the status of their correction.

The integrity measures associated with this activity are contained in Table 2.2-2.

2.2.43 Integrate System (Hardware and Software) AISF (Activity 2.43)

The system developer will integrate and test the system in accordance with the avionics systems integration plan. This will be done in an AISF and make use of the simulation facilities as the system is sequentially integrated.

A hot bench will normally be used to perform the system integration in the AISF. The hot bench is a complex combination of hardware and software with a number of aids available for use during checkout. Debugging aids of the hot bench center around software monitor capabilities.

Subsystem hardware and software verification and validation can be performed on a hot bench system. The LRU and embedded software are exactly the same as the equipment and configuration used within an aircraft. Assuming that comprehensive testing occurs, as required in the LRU test plan, validation of the LRU against the subsystem requirements can be achieved. At the very least, the results of hot bench testing can be used to add support to the results of the higher level simulation or flight test.

The results of each integration step and test should be documented in a system integration test report.

The integrity attributes associated with this activity are contained in Table 2.2-2.

2.2.44 Test System Integration in AISF (Activity 2.44)

This activity is normally conducted by an independent test organization in accordance with the systems integration/test plan. Failure modes and effects test are often conducted in each integration step by the independent test organization. Extensive use is made of the hot bench facilities in conducting these tests.

The types of tests conducted are designed to validate the sytem integration. Often these tests are of the form of the testability activities in RADC-TR-82-189 for the validation phase.*

_____

* Byron, J., Deight, L., Stratton, G. "RADC Testability Notebook"
  RADC-TR-82-189, Hughes Aircraft Co., June 1982

The independent test organization shall prepare a report documenting any discrepancies for each integration step and an overall report summarizing all discrepancies noted.

The integrity measures associated with these testing system integration are contained in Table 2.2-2 for this activity.

2.2.45 Integrate System into Aircraft (Activity 2.45)

Once the system integration tests in the AISF are complete, the system shall be prepared for flight test. The flight test aircraft is typically a test aircraft or an operational aircraft for which the avionics is designed that will be used for tests.

The avionics shal, be integrated into the aircraft as specified in the avionics systems integration plan. At each step of the integration, the interfaces all be verified as specified in the test procedures.

At the completion of the integration of the system into the aircraft, the results shall be documented in an aircraft integration report. Any anomalies or changes shall be entered into the system data base. Upon correction of the anomalies, the system should be subjected to the test sequence in which the problem was encountered and the data base updated to indicate the present status.

The integrity attributes associated with this activity are given in Table 2.2-2.

2.2.46 Develop System Validation Test Plan And Procedures (Activity 2.46)

The system validation test plan encompasses verification. The validation test plan should describe the techniques or methods to be used in the validation of the system. The validation test plan should specifically identify each of the selected test concepts which will be used for system level tests.

The validation test plan will contain the test objectives, and a description of the test environment, including required hardware and software, the delineation of the requirements being validated, and the evaluation plan. The evaluation plan will consist of the acceptance criteria and a description of the techniques to be used in analyzing the test data in order to determine compliance with the acceptance criteria.

Individual test procedures will describe the sequence for specific tests, the test input data, the data base, identify the software configuration, and identify the required test personnel and their functions.

Observations of the test itself and evaluation of the test output data constitute the basis on which it is determined whether the test objectives have been met, pertinent requirements validated, and the acceptance

criteria satisfied. The evaluation of the output data, if performed manually, is likely to be a tedious time-consuming process for all but the most elementary of tests. The manual task of error-checking is in itself an error-prone process.

The integrity attributes associated with this activity are given in Table 2.2-2.

2.2.47 Perform System Validation Tests (Activity 2.47)

The system validation tests are designed to demonstrate that the system will correctly operate in the environment it is designed to operate in and tolerate system transients and other faults the system was designed to tolerate. These independent validation tests may occur in the same time frame as a flight test performed by the aircraft manufacturer.

Any discrepancies or anomalies identified during validation will be documented and provided to the system integrator or equipment manufacturer as applicable.

The integrity attributes associated with this activity are given in Table 2.2-2.

2.2.48 Perform Flight Test (Activity 2.48)

The flight-test program is also part of the system validation process. The flight environment provides those unmodeled characteristics that are not included in ground laboratory test simulation. The hardware itself is exposed to simultaneous temperature, vibration, and operational situations which never seem to be covered in ground-test matrices. It is only in the vehicle itself that all the subsystems are in their true flight configuratio.

Should the flight test reveal a need for change in the hardware or software, the change would normally be made and validated in the avionics integration support facility as previously done before flight testing. At the completion of the flight test, a functional configuration audit may be performed on the software. The functional configuration audit "verifies that the CPCI's actual performance complies with requirements of the development specification". Data from tests of the CPCI is perused to verify that the item has performed as required. Requirements of the development specification not validated by the CPCI test are identified, and a solution for subsequent validation is developed.

An audit of the test plan/procedures is made and compared against the official test data, including checks for completeness and accuracy. Deficiencies are documented, and completion dates for all discrepancies are established and recorded. An audit of the test report is performed to validate that data accurately and completely describe the CPCI test. After the successful completion of the flight test program, the aircraft and its avionics normally enter an operational test and evaluation phase.

The integrity attributes associated with this activity are documented in Table 2.2-2.

2.2.49 Peform Operational Test and Evaluation (OT&E) (Activity 2.49)

The operational test and evaluation shall be conducted in accordance with the test plan. The objectives of the OT&E test are to determine the operational effectiveness and operational suitability of the system. The operational effectiveness portions of the test are concerned with capability of the system to perform its intended function in an operational environment while the operational suitability is concerned with the degree the system supports the mission and is maintainable. These tests are normally conducted by the end user. The results of these tests are used for identification of required modifications to the system hardware or software. The results are furnished to the system developer for use in correcting the discrepancies noted.

Table 2.2-2 contains the integrity attributes associated with this activity.

2.2.50 Production and Deployment (Activity 2.50)

This activity consists of the production of the quantities of the system required by the user, the acceptance testing of each system by the user, and the introduction to the operation of each of the new systems as they are delivered from the manufacturer. A full description of the manufacturing activities is contained in the following sections of this report.

2.2.51 Operation and Maintenance (Activity 2.52)

The user of the system must continue the configuration management activity.

As discrepancies are noted, they must be documented in order to permit correction. If manual methods are used to document these disrepancies, it is of vital importance that this information be recorded and furnished to the system developer. If manual records are not accurately kept, an alternative is to go to a computer aided identification and docimentation of discrepancies. While the development costs for a computer aided system might be significant, if the more accurate collection of data provides a timely correction of discrepancies, the cost may be warranted.

The integrity attributes associated with this activity are contained in Table 2.2-2.

REFERENCES - SYSTEM INTEGRATION PHASE ACTIVITIES ANALYSIS (2.2)

1.   (HANS82) Hanson, Jon G., "Design and Implementation of USAF
        Avionics Integration Support Facilities", AFIT/GCS/EE/81D-10, Air
        Force Institute of Technology, 1982.

2.   (ANGR74) Angrist, Elsa F., "A Survey of Avionics Simulation
        Facilities", MV-409-012-TAC/AFDAA, Federal Computer Performance
        Evaluation Center, August 1974.

3.   (HITT81) Hitt, Ellis F., Webb, Jeff, Lucius, Charles, Bridgman,
        Michael S., and Eldredge, Donald, "Handbook -- Volume 1, Validation
        of Digital Systems in Avionics and Flight Control Applications,
        "DOT/FAA/CT-82/115, Battelle Columbus Laboratories, December 1982.

4.   (HITT81) Hitt, Ellis F. and Broderson, Robert L., "Integrated
        Control Core Software Concept Study", AFWAL-TR-81-3141, Battelle
        Columbus Laboratories, December, 1981.

5.   (BYRO82) Byron, J., Deight, L., and Stratton, G., "RADC Testability
        Notebook" RADC-TR-82-189, Hughes Aircraft Co., June 1982.

2.3 MANUFACTURING PHASE: DESIGN COMPLIANCE AND PRODUCTION CONTROL

This section addresses the integrity aspects of manufacturing electronics hardware and identifies approaches and measures for achieving integrity.

Figure I-2.3-1 is the process diagram for the Manufacturing Phase: Design Compliance and Production Control. Those activities, identified in Figure I-2.3-1, include the efforts required to verify that the released avionics design meets all user-oriented requirements and that it is consistently and economically translated into finished product during the production phase of the acquisition cycle. Any failures which occur during this phase of development should be fully documented, diagnosed, and corrected prior to production.

This phase also includes the efforts required to verify that production quality is maintained throughout the manufacturing phase including transportation and storage (dormant reliability).

2.3.1 Management, Process, and Suppliers

Management, process, and suppliers are aspects of avionic integrity inherent to the manufacturing phase which cannot be shown in a process control diagram such as Figure I-2.3-1. However, they need to be considered and their impact on the integrity of the final product must be evaluated and taken into consideration early in the preproduction stages of the manufacturing process.

The criteria and measures of integrity are shown in Table I-2.3.1-1 for these three important aspects of the manufacturing environment.

The principal means, by which manufacturing activities are managed, are: (1) individual decision, (2) published schedules and plans, (3) configuration of factory organization, and (4) dissemination of policies and procedures. Company objectives and business plan are used to establish the principal control factors. If integrity is not stated in company policies, and not made an objective for evaluating performance, then integrity is difficult to deliver.

In order to insure that integrity is built into the final product, management should emphasize:

- Designs must be forgiving in all production systems in all environments.

- Parts/Material should have latent defects removed at the lowest level.

AVIONICS INTEGRITY PROGRAM (AVIP) PROCESS DIAGRAM
(SYSTEM/SUBSYSTEM)

MANUFACTURING PHASE:
DESIGN COMPLIANCE AND PRODUCTION CONTROL
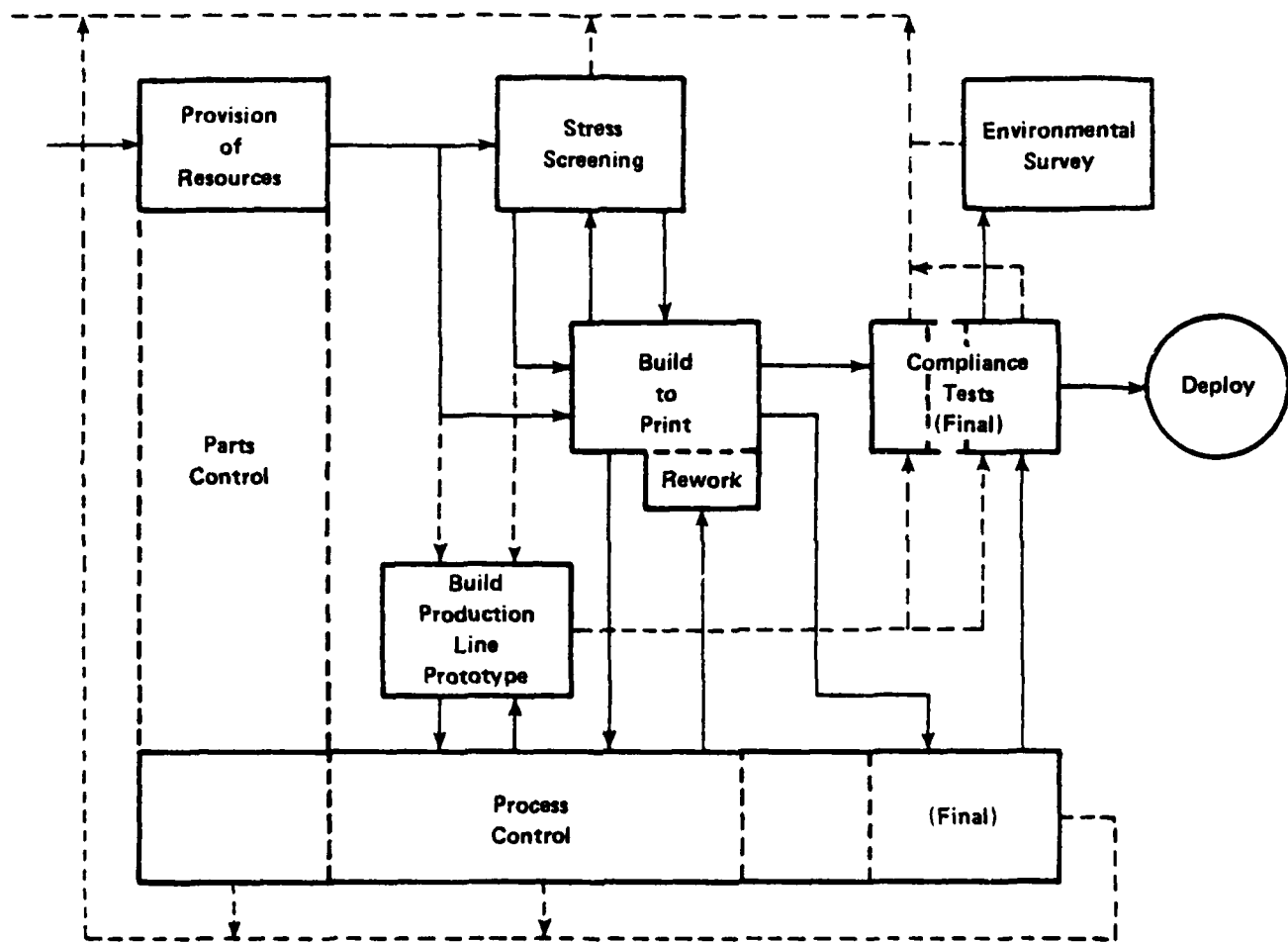
FIGURE I-2.3-1. Process Diagram

TABLE I-2.3.1-1. MANAGEMENT, PROCESS, AND SUPPLIERS COMMITMENT TO INTEGRITY

Activity	Sub-Activity	Integrity Parameters	Criteria	Measure
2.3.1 Management, Process, and Suppliers	--	Reliability Manufacturing Quality Quality Assurance Producibility Manufacturing Technology Assessment Lifetime (Durability) Maintainability	Management Commitment to Integrity	A. Integrity is stated in: • Company policies • Talks, day-to-day conversation of all management • Objectives of all management B. Assignment of authority and resolution of integrity issues versus performance issues
			Parts/Materials	λ Failure Rate
			People	A. Measured by the quality of product shipped/uniformity in process • Statistical quality assessments • Process control B. Measured by degree of support by people (management/labor quality circles, etc.)
			Process	A. Measured by the process control techniques which are elected and applied • Manufacturing quality • Productivity
			System	Measured by performance • Reliability • Availability • Dependability • Maintainability • Durability
			Pre-shipment Test Results	A. Measured by user specified, supplier performed tests
			User Performance Tests	A. Measured by user specified performance tests (i.e., stress screening, etc.)
			Supplier Involvement with User's Use of Supplier Product	A. Supplier involved with failure assessment and redesign B. User feedback to supplier

- Processes that cannot be controlled to the degree required, require understanding of how they fail and development of tests to recognize and find failures prior to their occurrence.

- People all want to make good parts, but you must tell them what they are doing wrong--plot and chart problems and provide feedback on the resolution of the problem.

From the process perspective, integrity requires interest, motivation and perseverance. A philosophy for obtaining integrity is presented in Table I-2.3.1-2(2).

Based on the above table (Table I-2.3.1-1) in order to enhance product integrity, it is necessary that specific management decisions be made and followed prior to, and during, the manufacturing phase. These decisions, which are initially made during the preliminary design phase, need to be re-evaluated in terms of production capabilities, goals and desires; and they need to be stated as management objectives. These decisions must (as a minimum) consider:

- Identification of worst case

- Ensuring that integral parts exceed worst case with margin

- Development of environmental stress screening for greater-than-mission profile where required to complement industry deficiencies to remove defectives

- Substantiation that all production equipment meet critical design performance characteristics

- Re-iterating that failure-free performance in environmental temperature cycling is a must

- Assessment of previous field failure data

- Assuring that the aircraft will not be the final production test environment. All possible infant and latent defects will have been identified and removed prior to development in the aircraft.

In addition to following the specific management decisions, the contractor's management must document what the company is going to do, the expected results, what was done to get there and, finally, record the actual results, compare them to the expectations, and correct any observed deficiencies.

Critical, of course, to all of this is building a system whose goal is to produce a cost effective product with high integrity in the identified environment, over the useful economic life of the system.

TABLE I-2.3.1-2. PROCESS INTEGRITY[2]

"Parts

- "QPL" only means the (parts) supplier had the formula once, it does not guarantee consistency

- Process control (for parts) cannot be maintained for desired military needs

- Environmental stress screen for known failure mechanisms.

Systems

- (Systems) do not fail, parts fail

- (Electronic systems) all use parts from the same suppliers

- (Systems) only fail when the design is not forgiving

- (Systems) need environmental stress screening for known failure mechanisms.

Reliability

- System requirements are more stringent than component requirements

- Environmental stress screen for known failure mechanisms.

Analyze Defectives

- All of the knowledge of what is wrong with a system is in its defectives

- Correct for defectives and you can evolve a perfect system

- Ensure corrective action through feedback systems

- Devise environmental stress screens for failure mechanisms.

Assess All Steps

- People process parts/material design

- "Quality is a state of mind that can be managed"

- "Use statistical quality assessments to test all production and enhance product integrity." (2)

2.3.2 Provision of Resources

Integrity is involved when resources are provided, trained, maintained and retired. When discussing integrity in the context of the Manufacturing Phase, compliance includes not only the procurement of materials and parts but also the necessary tools, production equipment, facilities and personnel. Each of these areas is discussed to illustrate aspects of integrity. The approaches and measures of integrity criteria due to provision of resources are shown in Table I-2.3.2-1.

Inputs to the resource provision activity come from the activities undertaken in the preliminary design, final design and integration phases, and result in the development of a production plan which covers the following subject areas:

- The business plan
- Master program schedules
- Ground rules and constraints
- Corporate organization and functional responsibilities
- Management systems
- Manufacturing parts list or bill of material
- Make or buy structure and subcontract management
- Manufacturing methods
- Logistics supports
- Engineering support of production
- Tooling philosophy, requirements and milestones
- Plant and equipment requirements and milestones
- Manpower requirements.

"The subjects covered in the production plan fall naturally into three categories: executive level plans and systems, manufacturing operations and other intermediate planning, and determination of detailed resource requirements.

"Executive level plans and systems encompass the Corporation's overall business approach, program master schedules, management ground rules and constraints, Corporate functional organization for program execution, and the management systems (and controls) to be applied. This category serves to convey management direction and guidance for the intermediate operations and detailed production resources planning which must follow."(6)

The management systems and controls, referred to earlier as a topic with the executive level of planning, are considered primary tools for program control, tracking, and detailed resource determination. Because the production plan activities begin early in a program it is important to have manufacturing represented in the earlier design phases.

"Manufacturing operations planning is best thought of as being the middle level of planning, between executive direction and detailed resources determination."(6)

TABLE I-2.3.2-1. INTEGRITY CRITERIA AND MEASURES DUE TO PROVISION OF RESOURCES

Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
2.3.2 Provision of Resources	Materials and Parts	Reliability Manufacturing Quality Quality Assurance Producibility Lifetime (Durability)	Transfer of Integrity Issues from Design to Production	Subjective--Judgment regarding rationale and practicality of user plans to transfer knowledge. Supported by past performance.
			Involvement of Suppliers in User Integrity Issues	Subjective--Judgment regarding where, when, and how user plans and does include suppliers in resolution of integrity issues, support by past user performance subject to supplier cooperation which should be documented.
			Identification of Part/Material Integrity Issues at Lowest Possible Level (Earliest Possible Time) with Confidence	Part/Material performance as measured in a variety of ways through production process from supplier screening through final test and analysis of field failures supported by past performance.
	Tools	Reliability Manufacturing Quality Producibility	Specified Tools Are Being Used and Replaced at Times when Integrity Is Being Affected	A. Subjective--Inspection periodically of production facility. B. Subjective--Review of plan and performance and tests for judging whether these are to occur. Equipment tolerances measured/compared with standard.)
	Production Equipment	Reliability Manufacturing Quality Producibility	Use of Specified Equipment, With Appropriate Calibration and Maintenance to Assure Integrity	A. Subjective--Production facility inspection. B. Subjective--Review planned and performed calibration, repair, and retirement. (Government has no authority to say when to retire equipment. It can see if there is a plan and the plan is followed and it can choose to not use equipment. It believes the integrity being promised is not met because of the use of a specific piece of equipment.) C. Subjective--Review data collection on equipment to see if it is being used according to plan.
	Facilities	Reliability Manufacturing Quality Producibility	Are Facilities Appropriate for Providing the Integrity Needed?	Subjective--Inspection of facilities looking for aspects which affect integrity issues such as cleanliness, work clutter, production line organization, etc. is it according to plan?
	Personnel	Reliability Manufacturing Quality	Worker Motivation to Fulfill Plan Integrity Efforts in Order to Achieve a Quality Product	A. Subjective--Judge whether user is performing personnel motivation as suggested in plan. B. Subjective--Identify level of worker participation and judge whether it is sufficient by looking at measures of quality, process control, and productivity performance erratic why.

The integrity activities associated with the procurements of materials and parts begins when materials and parts are being selected in the Design, Analysis and Development phases. From the administrative perspective it is important to the integrity program to assure a complete transfer to manufacturing of procurement information, design decisions and learned material and component nuances. Three common ways are identified:

- Transfer specification and design staff to manufacturing

- Temporarily loan manufacturing staff to design during final stages of design to learn and bring back the appropriate information

- Keep design and manufacturing separate except for problems, only specifications get transferred. (This technique is usually more common and least effective.)

It is important for suppliers to be involved in establishing and maintaining integrity. Suppliers' selection should be commensurate with their abilities to provide resources of the quality and of a price that will provide integrity. Cooperation and open communications with feedback on performance is effective in providing quality. Thus, communications with suppliers and personal interest in their efforts are the main tools for action. Good rapport with suppliers can provide the extra benefit of additional expertise (from suppliers) being available when a problem occurs in production. Further such good rapport makes buyer and supplier conflicts easier and usually more productively resolved.

From the perspective of provision of materials and parts (at the process level), integrity can be affected by late deliveries, improper handling and/or storage at receiving and improper delivery to the assembly line or work stations. The following examples illustrate how integrity can be affected:

- Late Delivery: Can force the manufacturer to buy from another source whose parts are by specification the same part but in actuality not of the same quality. This can occur because for the limited quantities needed in a short time; the extensive preliminary testing and evaluation may have been overlooked or deleted.

- Improper Handling and/or Storage: Parts and subassemblies have been shown, at times, to receive more severe temperature cycles or physical shocks during shipping and transfer than those specified for the system.

- Delivery to Assembly: Some components require very special handling, such as those requiring special handling to avoid electrostatic discharge.

The following procurement activities also need to be addressed at the "Materials and Parts" process level:

Vendor Survey/Approval
Purchase Order Reviews
Audit
Receiving
Source Inspection
Vendor Rating

Integrity can be very subtly affected by the tools being used in the production of high quality equipment. Administratively a company needs to be interested in whether the right/best tools are being utilized to produce the best product. Further, management should be concerned with providing tools in a timely manner so excessive wear or degradation does not gradually reduce product quality or affect the long term life of the product. A reporting system related to these facets of operation needs as much attention and action as do the reports on product qualification testing. At the process level attention needs to be focused on whether the design and specification of appropriate tools is in reality providing the appropriate or desired results in the actual manufacturing process. This further requires an understanding of tool wear and degradation on product quality. Finally, at the process level the individual(s) doing the work have to have an effective mechanism for conveying potential tooling problem situations (i.e., feedback, analysis forms, evaluation forms, etc.).

Suppliers of tools have to learn the problems their tools can cause for their users. Alternatively, they have to learn how to make a consistent product. If significant changes are made in producing the tools then the tool manufacturer needs to inform the user. What may appear to be a benefit to the tool manufacturer may turn into a significant quality control problem for the user.

Integrity is influenced by production equipment. Appropriate production equipment needs to be available, have scheduled maintenance, be properly calibrated and be retired in such a way as to maintain profitability yet provide the integrity and productivity required in the product. This is a particularly difficult challenge to electronic businesses today because of (a) the rapidly changing state of the art in electronics, (b) the introduction of automated equipment and (c) most currently the introduction of Computer-Aided Manufacturing (CAM).

Computer-aided manufacturing benefits the integrity of electronic systems. These benefits stem from the greater precision provided by automated systems and the automation of data gathering and data handling within the production environment. In addition, the flexible manufacturing system is set up by down-line loading from the computer-aided design system. Thus, the details for the manufacturing are communicated without error and thereby eliminate errors introduced by human operators. The automated data collection, data handling, and data processing of information from the production environment is now realizable with CAD/CAM systems. Such data collection and distribution provides instantaneous, periodic, or on-demand

quality data and feedback to the equipment operator, the production management, the operating management, and the quality assurance personnel. Intelligent sensor and on-line processors provide automatic and continuous quality inspection and feedback for control purposes, which allows for changes in process parameters to optimize the process for quality. A further benefit of data automation is continuous and effective product traceability and accountability from the physical inventory, as well as the quality assurance and quality test perspectives not previously possible with manual systems.

At the plant operations management level tactical plans for introduction of computer aided manufacturing systems must be developed in such a way as to minimize disruption to production, assure integrity, and guarantee optimum utilization of the human resources through active re-educational programs and specific programs aimed at optimizing integrity through automation.

From the operations point of view, the equipment supplier is a resource to the engineering, maintenance and procurement function. Operations Management makes decisions regarding vendors and specific equipment items. Maintenance and engineering functions must prepare for the introduction of CAM equipment by providing maintenance training for the people on the floor, system training for engineering staff and maintenance supervisors, and acquisition of any specialized skills required to support the process engineering maintenance function. In evaluating the vendors, close care must be taken to provide long-term support capability and the system supportability itself. Adequate provisions must be made for tools, maintenance equipment, test equipment, parts, and equipment and tools necessary to assure and verify the equipment performance. Preventive maintenance schedules must be established and organized with the vendor and executed by the maintenance staff to assure the integrity of the production equipment. A means for monitoring tools and measuring tool wear must be established and procedures for distributing and analyzing test results and production data must be established and put in place. Finally, both operations and maintenance management must assure that equipment repair and maintenance during normal usage is proper and the system performance is verified before being returned to the production process.

Integrity of the product may also be influenced by the facilities in which it is produced. First, they must be appropriate facilities. And second, modifying production areas and maintaining them can lead to the introduction of unknown, uncharacterized variables into the manufacturing process. This is also true of facilities which are deteriorating because of lack of maintenance. Therefore, it is necessary to establish a data collection activity to verify the performance of the facilities prior to returning them to the production process.

Integrity cannot be achieved if the personnel are not trained correctly and then properly motivated to apply what they have been trained to do.

A motivational program should not be based upon any one thing. "Rather, it is based upon the principle that people want to work and if their needs can be satisfied they will do a good job and can reach a level of

excellence. It is also based upon the recognition that human needs are dynamic, everchanging, and that management must be alert to new requirements as they develop." (3) Specifically, focusing on worker attitude, a program in which each employee is a catalyst by encouraging his or her peers, subordinates, and superior to improve product quality, is effective.

"The manifold costs of poor worker attitudes in the manufacturing process must be considered. First, there is an increased personnel turnover and the attendant loss of skill. Second, absenteeism increases as does the frequency and duration of work breaks for personal reasons. Absenteeism is a temporary loss of skill, which frequently requires the reassignment of work to others. This can be the cause of a partially completed process. Frequent work breaks cause a disruption of the thought process and loss of attention to detail which are deadly enemies to good workmanship. Finally, a disinterested worker has a greatly diminished attention span. His or her mind wanders back to items of greater importance at the time. Such losses of attention are the root cause for inspection escapes and missing steps in a manufacturing process. Depending upon the degree of worker disinterest, the result can be an acceptable product on one hand to complete disaster on the other." (3)

RCA (4) has put together a motivational program (including continuous management support and attention) which operates both within and outside the company to nurture and maintain motivation over a 10-year engineering development cycle of the AEGIS system.

The principal objectives of the program are to build and maintain a sense of involvement and team spirit among the participating companies and their employees. Public recognition is needed for firms and individual employees whose performance demonstrates a special awareness of the need for quality and productivity on AEGIS. The AEGIS Excellence Program provides:

- Individual Awards - Everyone involved in AEGIS is eligible. To date more than 200 individuals have been cited for outstanding performance.

- Contractor Awards - Top AEGIS program managers make special public presentations to firms (often small businesses) showing special awareness of quality and productivity.

- AEGIS Excellence Newsletters - 5,000 copies are circulated worldwide to ships and shore installations, Navy Department and other DoD organizations, and all involved contractors. This communication vehicle publicizes award winners and program progress, and provides the context for individual understanding of the size, scope, and importance of AEGIS.

- Poster - Widespread distribution and frequent updates provide a continuous visual reminder of the need for excellence in AEGIS.

"RCA has launched a derivative program, Involvement in Quality (IQ), to build an increased awareness of the need for quality and productivity and emphasize procurement as well as the manufacturing process.

"The IQ Program. The IQ Program specifically targets material suppliers and internal manufacturing operations for achievement recognition. In fact, IQ is a way of life, not merely a program. It has been comfortably merged into, and will remain a part of, the regular factory work pattern.

"The IQ structure involves awareness, information feedback, leadership, involvement teamwork, pride, recognition, achievement, and commitment. The initial effort, begun in early 1980, concentrated on procurement operations (suppliers) and moved gradually into manufacturing operations as the factory workload increased for AEGIS production. Project and engineering managers hold information exchanges with suppliers and with factory work teams. In the procurement area, special IQ awards are given to outstanding suppliers. Services are directed to helping vendors maximize efficiency and avoid potential problems. IQ in the factory has concentrated on group involvement, such as for small-group and individual-task development projects. Participation by factory personnel is encouraged by worker interviews (What's your IQ?) published with pictures in the RCA employee news magazine. RCA management participates actively in this effort.

"Another major thrust of the IQ Program is a team-building approach to factory quality, cost, and schedule control. The work-center concept involves a new look at organizational structure and the way manufacturing operations are conducted. Teams of people are brought together with all the essential skills and a sense of dedication for producing a reliable, maintainable product on schedule and within the prescribed cost parameters." (4)

"During the past 3 years, FMC Corporation's Northern Ordinance Division (NOD) has received $785,000 in Navy incentive awards for producing guided missile launching systems. Rather than pocket these awards as profit, FMC/NOD distributed the money to their employees to help generate enthusiasm for increasing quality and reliability in their equipment." (5)

These incentive awards are based on how well the launching systems have passed a demanding 24-hour operational test to measure system reliability. This test is the final demonstration in FMC/NOD's Reliability Acceptance Program (RAP). They have been effective in passing on 85 percent of the incentive awards to their employees.

Equitable distribution of the RAP awards among 3,500 employees is another sensitive matter. Many believe the program places too much emphasis on the one final RAP test and the work of the final test engineers, and not enough quality incentives for employees involved in earlier phases of the manufacturing process. FMC/NOD has tried three approaches to distribute the awards: (1) random drawings for merchandise, (2) drawings for $100 and $1,000 cash awards, and (3) general distributions which divide the RAP funds equally to all employees. An employee survey indicated that 76 percent favored cash drawings and general distribution, while 65 percent like the RAP drawings for merchandise.

"The most startling response came from the question, 'Has your work improved since the RAP began in order to improve quality and reliability?' While 44 percent of the employees surveyed answered yes, many felt that their

attention to quality was optimal regardless of the incentive program. Some reactions stated the motivation to work for quality and reliability should be a standard expected for a day's wage without addition cash incentives." (5)

2.3.3 Piece Part Control

Piece part control has become a critical issue in considering the integrity of the product during the manufacturing process. Even though screening and operating procedures have previously been established and formally passed to procurement and manufacturing after the critical design review, there are still several aspects that need to be addressed in the manufacturing phase. "Parts Control" can be considered part of the Provision of Resources (incoming inspection) and yet many of its aspects are nothing more than process control or compliance guidelines for the parts suppliers. The approaches and measures of integrity associated with Piece Part Control are shown in Table I-2.3.3-1.

The following activities are all considered part of Parts Control:

- Vendor Survey/Approval (trying to maintain multiple sources)
- Purchase Order Reviews
- Audits
- Vendor Part Qualifications (as vendors change or quality or product appears or is known to have changed)
- Receiving Inspection
- Source Inspection
- Vendor Ratings (feedback to vendor the impact of his product's quality on your production processes and product).

Effective parts control has been instituted by many organizations because of the number of faulty components being put in their product (Reference Table I-2.3.3-2). (7) In addition, the results of a questionnaire depicting the percent of parts received being defective is shown in Table I-2.3.3-3. (7)

The data in these two tables reflect the basis for a growing sentiment among electronics manufacturers toward initiation of improved parts screening. Further, the most significant force driving this trend is the dollar benefit received by replacing a component at the lowest possible level of identification (Reference Table I-2.3.3-4). (7)

In addition, the results from a survey of equipment manufacturers showing their estimates of cost to rescreen parts is presented in Figure I-2.3.3-1. (7)

TABLE 1-2.3.3-1. INTEGRITY CRITERIA AND MEASURES DUE TO PIECE PART CONTROL

Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
Piece Part Control	Role and Need for Parts Control	Reliability Manufacturing Quality Quality Assurance Lifetime (Durability)	Top level administrative review and support.	A. Subjective--Judge emphasis placed in planning document policies, organizational charts on integrity in parts control.
	Administrative	Reliability Manufacturing Quality Quality Assurance Lifetime (Durability)		B. Subjective--Authority assigned to resolving piece part control integrit issues versus other manufacturing issues.
	Process level	Reliability Manufacturing Quality Quality Assurance Producibility Lifetime (Durability)	Are screening procedures as planned being followed? Are they adapting to changes being made? Data collection regarding screening result with feedback to supplier.	Subjective--Inspection and judgment to whether plans are being fulfilled. A. Subjective--Judgment based on planned data collection and analysis activities are being performed according to plan. B. Subjective--Judgment based on inspection of user and supplier whether dat feedback on incoming screening is being performed and used.
	Supplier level	Reliability Manufacturing Quality Quality Assurance Lifetime (Durability)	Suppliers are fulfilling requirements.	User screening data and failure analysis compared to requirements of MIL-STD-883.

TABLE I-2.3.3-2[7]. PART QUALITY

Part % Defective	PWB Yield
2.9	5%
1.0	37%
0.5	61%
0.2	82%
0.1	90%
0.01	99%

Part quality must be better than
0.01% defective assuming 100 ICs
per board

TABLE I-2.3.3-3(7). PERCENT DEFECTIVE PARTS

Screening Level		IC's	Transitors	Diodes	Hybrids	Capacitors	Resistors
Higher than QPL	Lot Size	500,000	1,000,000	10,881,000	5,000	3,000	
	% Def.	2.3%	2%	.4%	5%	.3%	
QPL/Military	Lot Size	126,030,000	38,500,000	13,240,000	12,000	7,562,000	5,104,000
	% Def.	5.4%	3.8%	4.42%	7%	1.1%	2%
Higher than Comercial	Lot Size	8,000,000					
	% Def.	53.6%					
Commercial	Lot Size	5,042,000					
	% Def.	1%					

All numbers expressed in 000's.

Maturity of parts 95% of all cases exceed 5 years.

TABLE I-2.3.3-4[7].   PART REPLACEMENT COST

Component	PWB	WRA	System	Field
$5	$50	$500	$1,500+	$15,000

Lowest cost - find the problem at the part level.

44% OF REPORTED COMPANIES SELF IMPOSED SCREENING

Screen Costs	$.15-$4.00	$.10-$3.00	$.10-$3.00	$.15-$1.00	$.02-$1.00	$2.00-$15.00
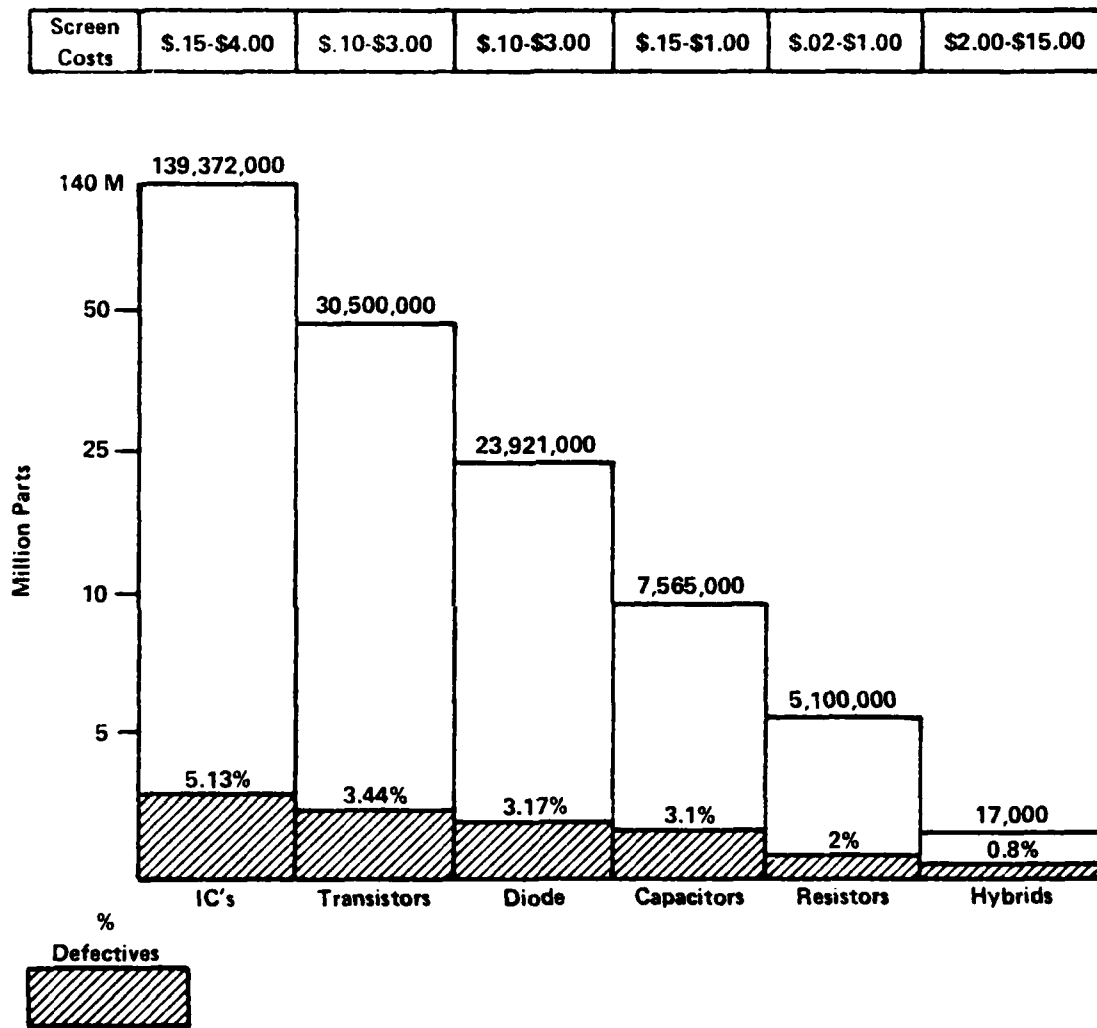
FIGURE I-2.3.3-1. Equipment Manufacturer's Screen Results and Costs

Based on the data in Table I-2.3.3-3, Figure I-2.3.3-1, and other related studies, equipment manufacturers have begun to institute rigorous piece parts control programs. Litton, as an example, based on experience similar to this, became "dissatisfied with the failure rates of assemblies and systems during in-process and final test, and management decided a strong control program was necessary. After proving 70 percent of the failures in production were directly attributable to deficient electronic component parts, we discovered that screening out component part failures at receiving inspection is more cost effective than finding these failures during assembly or system level testing. Spending pennies at the part level saves dollars and should save time at the higher levels. In addition to these cost savings, less rework at the assembly levels now gives Litton's system a higher overall reliability. It should be apparent to manufacturers of military electronic equipment that the less a system or module is reworked, the greater its probability of performing satisfactorily during its intended life cycle. These various factors prompted Litton management to proceed with a plan to revolutionize its receiving inspection and place heavy emphasis on control of its suppliers." (1)

Similarly, Westinghouse (1) has made the following conclusions about parts control:

"• One hundred percent testing of all incoming electronic parts is unnecessary.

• Experience at Westinghouse shows that the level of quality for resistors, capacitors, and diodes is satisfactory. For these parts, extensive use of acceptance sampling is adequate to control the quality of parts received from vendors.

• For semiconductor devices with today's quality levels, there is a need to 100 percent screen all incoming parts because of the impact on factor yield the first time through the process.

• Incoming screening of electronic parts is the lowest cost way to find defective parts.

• Although the cost of an IC Tester is high, the return on investment justifies the capital expenditure.

• More comprehensive incoming part testing is needed including ac, dc, functional, high, low, and ambient temperature and burn-in.

• High speed data logging on a computer must be coupled with digital and analog IC Testers to provide more test intelligence.

• Until the level of semiconductor quality improves dramatically, the incoming screening of parts is the proper business decision." (1)

The Westinghouse conclusions were based not only on their parts experiences but on an investigation of the existing MIL-STD quality

conformance requirements. Based on their examination of MIL-STD-883, Westinghouse concluded:

"It is assuring to know that semiconductor parts have been purchased in accordance with military specifications such as MIL-STD-883. However, a check of the quality level specified is not good enough based upon the PWB yield analysis. Figure I-2.3.3-2 is a sample quality conformance test extracted from MIL-STD-883 and indicates lots with 5 to 10 percent defective material should be accepted 10 percent of the time and lots with 1 percent defective material approximately 90 percent of the time. Although semiconductor manufacturers regularly comply with this specification, the quality of the material is not good enough to achieve high-process yields because 90 percent of the time material which is 1 percent defective can be shipped." (1)

Subgroup	Test	Level B* LTPD***	Level S* LTPD
1	25 C Static	5	5
2 and 3	Hi and Lo Temp Static	7	5
4	25 C Dynamic	5	5
5 and 6	Hi and Lo Temp	7	5
7	25 C Funct	5	3
8	Hi and Lo Temp Funct	10	5
9	25 C Switching	7	5
10 and 11	High and Low Switching	10	5
	0.01% Defective Required		

*Level B--Normal Military Application
**Level S--Space Qualified Parts
***LTPD--Lot Tolerance Percent Defective

FIGURE I-2.3.3-2. Sample Quality Conformance Test(1)

The above studies and conclusions reinforce the need to establish and maintain a rigorous piece part control program which will provide the best product at the least cost. Such a program can generate additional front end costs due to the cost of the higher quality parts (i.e., manufacturing costs, test screening costs, documentation costs, data collection costs, etc.). However, if a rigorous program of piece part control is established, managed and maintained from the earliest design phases to the final production phases, then it can be inferred that integrity will be built into the product and that the reliability goals will be achieved.

2.3.4 Process Control

The process control activity interfaces with all aspects of manufacturing and can extend back into the development process. The process control activity controls the planning and physical production in product delivery while simultaneously generating the required reports, qualified vendor lists and quality related schedule and budget change requests. The process control activity generates process and inspection plans as are required and approved in a Production Readiness Review. It is concerned with component source control, incoming inspection, assembly control, workmanship specifications and standards, quality/productivity improvement and manufacturing efficiency. Because of the major role process control plays in the manufacturing process as a whole it is also concerned with the introduction of automatic test equipment and computer-aided manufacturing. Figure I-2.3.4-1 indicates some of the far reaching influence of Process Control (in this figure reflected as QA) and Table I-2.3.4-1 shows the approaches and measures of integrity criteria.

Process control specifically with respect to integrity aspects has been undergoing significant improvements with the implementation of MIL-Q-9858A and the institution of statistical quality control techniques to control product quality characteristics.

The introduction of automation and computer-aided manufacturing will change the complete nature of the type of work and the types of interactions that the process control staff will have with manufacturing. Current process control emphasis is on characterizing the process by measuring the product. It is important to note that this concept does not imply a simple sorting operation. With currently used statistical quality control techniques, product characterization is very effective. There appear to be two cases where this approach will not be effective (11):

1. The first is where the process under consideration is flexible automation. "Flexible systems lend themselves well to short runs. Such short runs do not always leave enough time to acquire the measurements needed to satisfy statistical requirements. Furthermore, flexible systems often involve the production of very wide part mixes." (11) Another problem in this case involves the seamless aspect of automated processes, where one operation flows into the next without any break, thus preventing the insertion of the measurement operation.

TABLE 1-2.3.4.1 INTEGRITY CRITERIA AND MEASURES DUE TO PROCESS CONTROL

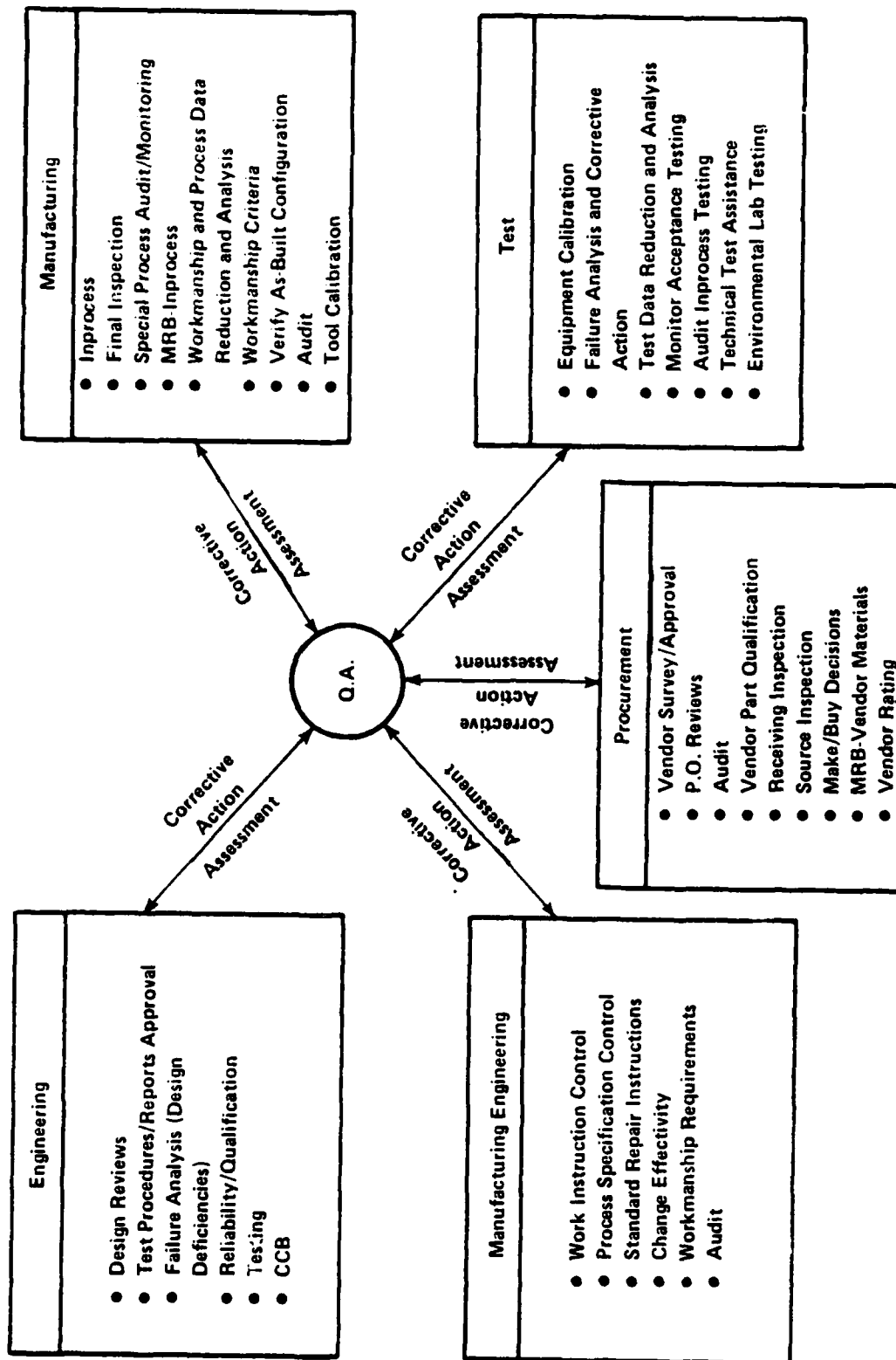| Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
Process Control	Introduction	Manufacturing Quality Quality Assurance Manufacturing Technology Assessment	Utilization of process control techniques and tools is planned.	A. MIL-Q-9858A. B. Compliance with planned activities including analysis and timely action taken to correct.
	Planning/Documentation Related to Control	Reliability Maintainability - Supportability - Testability - Reproducibility	Documentation or process control results.	A. Inspection to determine the documentation is being done in a timely fashion according to plan. B. Subjective. Are the results of process control being used effectively and in accordance to plan?
	Information System	Manufacturing Quality Producibility Manufacturing Technology Assessment	Use of the information systems planned.	A. Subjective--judgment about use and usefulness. B. Compliance to plan.
	Statistical Control Techniques	Reliability Manufacturing Quality Producibility	Effectiveness of the planned process control techniques.	A. Amount of rework. B. Yields as a whole.
	Computer Aided Manufacturing	Reliability Manufacturing Quality Quality Assurance Producibility Manufacturing Technology Assessment Maintainability	Computer-aided manufacturing providing the benefits identified in the proposal and operation according to plan.	A. Measure of costs to produce that associated. B. Process control data. C. Quality performance data. D. Failure analysis assignments to the computer-aided manufacturing equipment.
	Production Readiness Review	Manufacturing Quality Producibility Manufacturing Technology Assessment	Is manufacturer ready to produce?	Subjective--Government accepting company production plans and giving go ahead to produce
	Component Source Control	Reliability Manufacturing Quality	Control of component sources to insure continuously available throughout production the required amount of components.	A. Multiple qualified part source. B. Subjective--judgment of whether suppliers are adequate sources based on review of the vendor ratings. C. Subjective--judgment of suppliers (facilities, personnel situation and financial position--usually considered acceptable if supplier has been certified acceptable
	Assembly Control	Manufacturing Quality	Consistency in control measures.	A. Are they within planned variance? B. Subjective--Are frequency and amounts of being indicative of a problem? C. Generation of excess waste materials to achieve integrity. Is waste within planned amount? D. Subjective--what is waste resulting from and does that reflect on an integrity issue?
	Workmanship	Manufacturing Quality	Are the workmanship standards planned being employed?	A. Subjective--Discussions with employees about their work and use of standards. B. Analysis of a sample product to verify use of standards.
	Incoming Inspection	Manufacturing Quality Quality Assurance	Manufacturing disciplines are operational. Quality improvement. Use of analysis.	A. Continuous process and product audits. B. Quality yield charts. Subjective--trend lines in yield charts of amount of rework? A. Subjective--what and when does it happen when rework and yield charts show uptrend? B. Does the same integrity issue reoccur based on analysis?
	Manufacturing Efficiency Program	Manufacturing Quality Producibility	Is incoming inspection plan providing the part quality needed to meet system performance requirements? Reduction of rework and reject rate improves integrity.	A. Failure analysis indicating whether failures are problem due to inadequate inappropriate testing. A. Chart amount of rework and reject rate each level. B. Subjective--judgment regarding upward trends in the rework charts.

FIGURE I-2.3.4-1. Quality Interaction

"Therefore, one must either interrupt the process, which reduces the productivity gains of automation, or wait until the completion of a station's operation, thus risking the high degree of value added at that station. As increased performance requires the use of more exotic, high unit cost materials, the latter option becomes even less desirable." (11)

2. "There is a second case--even more problematic--for which it is not possible to establish a tight cause and effect relationship between a product attribute and a process variable. Such cases include truly random events such as faults in a silicon chip or specks of dust on a photomask." (11)

"In the future, NBS (National Bureau of Standards) believes that the predominant quality control strategy will involve direct process control--not the measurement of product attributes. This 'make it right the first time' philosophy will depend on a concept gaining credence at NBS called 'Deterministics Metrology'. This concept is based on the premise that future automated manufacturing environments will incorporate precharacterized, uniform incoming materials and a well-understood process that permits valid predictive modeling. This strategy will make it possible to monitor the process in real time and prevent the production of a bad product." (11)

Another author (14) not only sees the changes as highlighted above, but also sees two others becoming important. For the sake of another perspective, Keeler (14) describes his two approaches to control in the following way:

"There are two approaches to inspection for process control today. The first, which is termed 'in-process' inspection, has been perfected over the past forty years or so, and relies on a human inspector to sample product coming out of a process unit. The inspector keeps graphical records known as control charts which describe the state of the a process and help to track any tendency of it to drift. Although it is low-tech, it has proven to be a astonishingly successful tool in the hands of manufacturers." (14)

The second approach is quite new and holds the promise of almost total accuracy while doing 100 percent inspection. It is on-line inspection and it entails automatically checking one or several physical parameters of the product or tool, then storing the data acquired in real-time in the memory of a computer (Hence the term "on-line") and converting the data into useful information for decision making. It may also offer the capability of information sharing through linking up with other inspection stations in a local area network.

The discrepancy between Simpson's (11) and Keller's (39) descriptions lies in describing the second approach. Keeler allows for

automatic testing of the product and Simpson does not. A second trend seen by Keeler (39) is that there is a shift of emphasis toward manufacturing process control and away from final test in the printed wiring board industry. "The other is the intriguing idea that if you can help your supplier get his process under control you might be able to eliminate your own incoming inspection function. In both cases, in-process inspection is the tool which can inform the manufacturer whether or not his manufacturing process has gone awry." (39)

In all cases the general impression with respect to Process Control is that the contractors are finding it is cost effective to build the product right the first time. Table I-2.3.4-2 attempts to identify some of these cost trade-offs.

TABLE I-2.3.4-2.THE COST OF NOT DOING IT RIGHT THE FIRST TIME[14]

Expense of failure	Expense of appraisal	Expense of prevention
Scrap	Engineering time spent in preparing specifications	Engineering effort
Rework and touch up		Reliability evaluation: burn-in testing, etc.
Troubleshooting	Incoming Inspection	R&D time: Anything done to reduce costs of failure and appraisal
Engineering time	Inspection in progress	
Warranty servicing	Q.C. monitoring	
Loss of goodwill in the marketplace	Final test	
Other	Other	Other

This section of the process control discussion will not attempt to enumerate the large number of documents and database systems which could be applicable to this subactivity. It will only highlight some of the more familiar ones and emphasize the need to document those things for which a definite use is known. (Do not collect, store or document information for

which there is or will be no use.) Planning and documentation related to controlling production used for interfacing with engineering and manufacturing engineering to help develop, get approval on, retain and insure fulfillment of such documents as:

- Controlled working environment
- Controlled production equipment
- Test procedures
- Failure analysis reports
- Reliability/qualification information
- Work instructions
- Standard repair instructions
- Audit reports
- Final inspection results
- Tool calibrations
- Special Processes Audits
- Test data reduction
- Acceptance test results
- Environmental tests results
- All manufacturing, testing, process control documentation
- Process control.

Because of the magnitude of information to be handled, a clear labeling and index system for rapid identification and retrieval is necessary.

Information Systems are used by many companies and are important for integrity. For example, "Two of the more significant management systems are the Program Management Information System (PMIS) and the computerized Manufacturing and Planning System (MAPS)". (6)

"PMIS is the Corporate system wherein a plan or baseline is established; progress is measured, reported, and compared against the baseline; and appropriate action is prompted whenever a comparison indicates an actual or potential problem. To serve as an adequate basis for responsible decision making, the PMIS provides timely, valid, and auditable data related to cost and schedule accomplishments. While this system is committed by Corporate management for program administration in the production plan, it is essentially a tool for program execution.

"MAPS, the other major management system, is valuable in both production planning and subsequent program execution. MAPS uses, and is supported by, a number of interrelated systems or subsystems used in the production planning process. These include the work measurement system, the lot plan and release system, the lead time system, and master scheduling for manufacturing." (6)

Another useful system is the End Item Data Package (EIDP). Briefly an EIDP is a concise compilation of rework events occurring on a single serialized end item throughout its manufacturing and test history. When these data are plotted, the result is a graphic illustration of the variability innerent in the manufacturing process. The initial objectives for EDIPs were:

● To provide visibility of the contractor manufacturing process variability

● To monitor the overall effectiveness of the contractor product assurance program

● To provide an early indication of the product readiness for fleet use.

Process control is also responsible for the development of existing statistical control techniques, the most important of which are presented in Table I-2.3.4-3.

Another activity of component source control is related to vendor rating and is fairly specific to defense electronics. "The activity requires the development of vendor requirements, the accumulation of a vendor history and the development of vendor ratings in comparison to the performance against their requirements. This function supplies a qualified vendor list to the procurement activity. It is anticipated that the accumulation of historical data and reporting of vendor ratings will be supported by a computerized information system supportive of the defense QA information require- ments." (15) Also there is "Vendor Audit: The inspection of a supplier's facility to determine if he has the long term capability to provide a commodity that meets the specification. And Vendor Certification: A statement of approval for a given supplier, based on the confidence gained during a vendor audit that he can and will comply with the requirements for quality, and will supply documentation proving process control." (14)

"The requirement for component traceability within defense elec- tronics is unique to that industry. The function must track assembly data, subassembly data, and provide component traceability data of compounds to their sources so that any difficulties that develop throughout the life cycle can be traced to an individual vendor or lot of components. The function is controlled by materials specifications, engineering design data, quality assurance plan and the contract requirements. It operates from historical component data and delivers the component product traceability data as required by the contract and performance costs and schedule reports for the function itself to factory management." (15)

Assembly control is concerned that "fabrication and assembly opera- tions shall be controlled to assure that characteristics specified in the applicable technical documentation are consistently achieved and maintained in the produced items. Sources of wasted effort and material caused by work not done right the first time will be identified and eliminated." (8)

Those aspects of process control "which supports production, inspec- tion and test contains three primary identifiable functions. These are the development of test and inspection plans, the auditing of the process and inspection instructions, and the development of test equipment calibration procedures. The activity is expected to produce the required process inspection plans and manufacturing instructions as well as test equipment calibration data and related cost status reports. The inputs and controls are

TABLE I-2.3.4-3.[14] STATISTICAL CONTROL TECHNIQUES

"AQL: Acceptable Quality Level. Expressed as a percentage, it means the maximum portion of defective product that will be tolerated in a given lot.

C-chart: A control chart for attributes (i.e., go/no-go data) showing the number of defects per sample taken.

Check sheet: A data collection form that covers most of the defects an operator will encounter. It may describe the nature of the defect, its location, the quantity found, and the manufacturing environment at the time.

Control chart: A graphic record for evaluating the consistency of a process over a period of time.

Control limit: Limit on a control chart for judging whether or not a statistical measure obtained from the sample falls within acceptable bounds.

100 percent inspection: The inspection of every unit of product that passes through a work unit or through final inspection. It is never 100 percent accurate when human operators do the inspecting, because of sense limitations.

Pareto diagram: Usually in the form of a histogram, it plots defects against frequency of occurrence. It often shows that approximately 80 percent of quality problems stem from just 20 percent of the defects. It is a tool used to prioritize the most important problems and has applications in many fields, not just quality control.

P. chart: A control chart for attributes showing the percent of defective product per sample taken.

Sampling plan: A procedure for selecting items and determining whether the quality level of the source of the sites is acceptable; it takes into account any random variation.

X-bar and R chart: A control chart with control limits based on average (X-bar) and range (R)." (14)

historical performance data, engineering product description, the quality assurance plan, the manufacturing process plan, and manufacturing instructions." (15)

Also to be considered under assembly control are the working conditions. Control of such things as lighting, humidity, temperature, CRT screen glare, etc., improves integrity, reduces contaminating sources and aids in producibility.

2.3.5 Production Line Prototype Fabrication

The production Line Prototype (PLP) Fabrication activity occurs as early in the manufacturing cycle as possible. It is critical to operating a smooth successful production line to have the PLPs be built with the same tools, processes, etc., as are specified and would be used in full production. The PLP activity and its product are used to validate the process controls, stress screening, and compliance test activities.

It is also very important to understand that the PLPs are significantly different from those made in the laboratory. First, the units produced in the laboratory are typically all hand constructed by very skilled people dedicated to making things work right the very first time. They use skills, tools and tricks they have learned from many years of building laboratory models to make units function well. Second, the laboratory units are made by hand wiring, wire wrapping and special quick fix connectors. These types of processes will not adequately reflect unit performances under the testing that must be attempted on the PLPs. Laboratory units typically do not have their parts qualified as they would be in production. Therefore, it is not advisable to use laboratory units as PLPs, the practice can lead to erroneous test results causing needless delays and redesigns. Use PLPs which truly reflect the production process and environment. The approaches and measures of integrity criteria are shown in Table I-2.3.5-1.

From an administrative perspective it is useful to encourage as much cooperation as possible from the production staff to make these units like production units using the specified manufacturing procedures. It is with these PLP units you should expect to be spending a considerable portion of your time resolving conflicts, procedures, domain differences, refining and getting approved revised specifications and resolving the general havoc of setting up a production process. The more emphasis you can place on having a quality product and the more persistence you have in reaching solutions toward providing that type of product now, the easier your job will be over the long haul in administering the production. Attention is needed to details of parts failure and correspondence to anticipated types of failures. Providing real and long lasting solutions to these problems now pay extremely high returns in production. You need to have the best design people and electronic pathologists at your disposal during this time to resolve problems. Lastly, be sure there is documented those areas where the PLP units will differ from normal production hardware and from normal production processing. It will be these areas in production start up that will require some initial attention.

I-97

TABLE I-2.3.5-1. INTEGRITY CRITERIA AND MEASURES DUE TO PRODUCTION LINE PROTOTYPE FABRICATION

Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
Production line Prototype fabrication		Manufacturing Quality Quality Assurance Producibility	Difference between production line prototype and real production line product and impact of integrity.	Subjective--Identify differences and assess impact testing has, compensate to provide for integrity and verify at earliest opportunity.
			Staff cooperation with concern for achieving realism to be able to assess integrity issues.	Subjective--Judge concern and involvement of staff doing this task.

2.3.6 Stress Screening

Stress screening is used to identify weak aspects of a system at the lowest level of assembly. Stress screening can be used both with parts and assemblies and during the process of building both the production line prototype and the actual products. Results of the stress testing should be feedback into the process. Failure rate data can be used in process control while diagnosis of the failures can track whether the test is achieving its intended objective and whether the prior processing is under appropriate control. The approaches and measures of integrity are shown in Table I-2.3.6-1. (In addition to the material presented here, Appendix I-A-4 contains technical material related to Environmental Stress Screening which is of value in understanding the role of stress screening in obtaining a product that has integrity.)

"Due to the varied nature of military electronics equipment and their associated design and manufacturing program characteristics, it is difficult to "standardize" on a particular screening approach. A tailoring of the screening process to the unique characteristics of a given program is, therefore, required. Screening methods such as a temperature cycling and random vibration appear to be the most effective for removing part and workmanship defects. However, exposure levels, number of cycles, and durations of screen application differ widely among users. Other, perhaps less costly, screens such as sinusoidal vibration, power cycled burn-in at ambient and temperature soak are also used, but, in general, their effectiveness is believed to be less than the former tests." (13) A reasonably precise data base on the effectiveness of the various available screening tests is currently being established. Screening techniques therefore, should be selected based upon effectiveness, early development program data and on hardware design, manufacturing, material and process characteristics. "The screening process then, should be continuously monitored and test results analyzed so that changes in the process can be made, as required, to optimize the cost-effectiveness of the screening program." (13)

"The purposes of environmental stress screening should not be confused with those of production reliability acceptance tests, reliability demonstration tests, mission profile testing or qualification tests. All of the former tests are performed on equipment samples only, for purposes of verifying compliance with design or lot acceptance requirements. It should also be noted that tests, such as mission profile testing, seek to simulate mission environmental stress conditions whereas environmental stress screening is aimed at the precipitation of (weakness or) defects using efficient screening procedures which provide a maximum of screening effectiveness with a minimum expenditure of time and resources." (13)

"A key goal of a stress screening program should be to bring about its own obsolescence. A screening program established at the beginning of a production program should not be continued unchanged throughout the duration of the production contract. Such practices can result in high costs to the government without adequate knowledge of the benefits being gained from the screening program. It may be necessary to increase stress levels or change

TABLE I-2.3.6-1. INTEGRITY CRITERIA AND MEASURES DUE TO STRESS SCREENING

Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
Stress Screening	Reference Appendix I-A-4	Reference Appendix I-A-4	Removing defects and latent defects as the lowest possible assembly level.	A. MTBF MTBR Lifetime B. Failure analysis of components--are you missing some latent defects? Are you introducing defects due to the production process?
			Cost-effectiveness of stress screening.	A. Number of part failures obtained at higher assembly testing. B. Number of board level failures obtained at higher assembly level testing. C. Types of field failures.
			Is stress screening percipating expect number and types of defects	Failure analysis results. Subjective--Judgment comparing results to expectations.
			Is stress screening needed?	Subjective--Judgment based on defects participated during failure analysis experiment.

stress types if latent defects are found to be escaping the screens. It may also be advisable, from a cost standpoint, to discontinue or relax certain screens when the production process matures, i.e., when process controls and corrective actions have been established or taken to reduce the defect population to acceptable levels.

"Provisions should be established to monitor and analyze the screening process so that results can be used to take the necessary corrective actions to remove root causes of the defects from the production process. The cost-effectiveness of the screening program should also be tracked so that decisions, trade-offs, adjustments can be made as the program progresses to maintain the stress screening program at maximum cost-effectiveness. Without such provisions to ensure that the screening program is cost-effective, the screening process can become an open-ended and costly exercise with greatly reduced or negative benefit.

"The development and production contract should contain requirements for, and provide the flexibility which allows the contractor to optimize stress screening plans. An evaluation of screening effectiveness and costs should be required to be performed on a representative sample of (production line prototype) hardware prior to full scale production. The hardware should be characterized in terms of design and production process variables in order to generate the inherent defect population data required for screen selection and placement in the production process. The contractor should be required to propose a stress screening plan to be reviewed for acceptability by the procuring activity prior to full scale production. Contracting arrangements should be used which allow change to be made to the screening program in order to maintain it at maximum effectiveness." (13)

A proposed military standard on environmental stress screening MIL-STD-XXX is available and should be referenced when performing the actual work in this area.

"Stress screening programs offer significant potential for improving field reliability and reducing both production and field repair costs. Figure I-2.3.6-1 below models a production process and shows a typical range of costs for repair/replacement at each assembly level. The costs of repair in the field are also shown in the figure.

"Two important points must be kept in mind in carrying out a stress screening program. The quantitative aspects of stress screening, i.e., the expected number of defects and the ability of a specific screen to precipitate those defects are not known with certainty. Past experience may provide some guidance in cases of similar equipment composition, construction and degree of production maturity. It must also be determined if a stress screening program is appropriate. Screening may not be required on mature production programs. If the quantities of defects are expected to be low, then a stress screening program may not be necessary or cost-effective. Once a decision has been made to use stress screening, however, then the screening program should be tailored to the unique characteristics of the hardware design and production process. A cost-effective analysis should be performed in conjunction with the tailoring process in order to provide assurances that maximum screening effectiveness is obtained at minimum cost." (13)
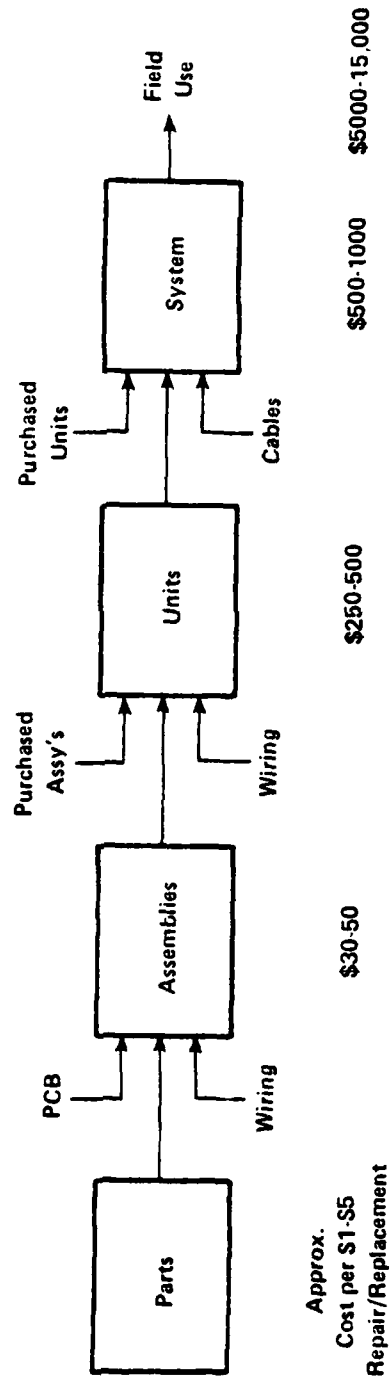
FIGURE I-2.3.6-1. A Typical Production Process

The proposed experimental stress screening MIL-STD should be consulted regarding specific requirements.

"Estimates of the type and quantity of defect likely to be present in the hardware are essential for properly tailoring a screening program. Past experience with similar equipment may be helpful in making such estimates. Once defect types have been identified then the stress conditions most likely to precipitate the defects can be selected. Stress type, level, duration and method of application must be determined. The following sections provide guidance on some of the key issues which must be considered in planning and tailoring a screening program.

"Both part and assembly defects are introduced during the fabrication, assembly and test of electronic equipment during manufacture. Some of the defects may only require a functional test of sufficient thoroughness or a visual inspection, in order to detect and eliminate them prior to shipment. Such defects can be termed patent defects to distinguish them from latent defects. Latent defects cannot be detected by ordinary means and require stress over time in order for them to be degraded to a detectable level. Some examples of latent defects are:

Parts

- Broken or damaged in handling
- Wrong part installed
- Correct part installed incorrectly
- Part failure due to electrical overstress (EOS) or electrostatic discharge (ESD)
- Missing part

Interconnections

- Incorrect wire termination
- Open wire due to handling damage
- Wire short to ground due to misrouting or insulation damage
- Missing wire
- Open etch on PWB
- Open plated-through hole
- Short Etch (solder bridge, loose wire strand)

"Some examples of latent defects and the type of screen believed to be effective in precipitating them are provided below: (Table I-2.3.6-2)." (13) "In evaluating screening process fall-out data and screen effectiveness, care should be exercised to distinguish between screen-related latent defects and patent defects. The use of pre-screen testing, which is discussed later, is recommended during early production as an aid in evaluating screen effectiveness." (13)

"A stress screening program conducted during a development or early production phase will be concurrent with many other product improvement activities such as design changes, manufacturing process changes or supplier corrective action programs. These simultaneous activities will collectively

TABLE I-2.3.6-2.[13] LATENT DEFECTS

Defects	Thermal Screen	Vibration Screen
Parts		
Latent material and process defects	x	x
Partial damage through EOS/ESD	x	
Partial physical damage in handling	x	
Improperly installed part	x	x
Interconnections		
Cold solder joints	x	x
Inadequate/excessive solder	x	x
Broken wire strands	x	
Insulation damage	x	
Loose screw or wire termination (lugs)	x	x
Improper crimp	x	
Unseated connection contactor		x
Cracked etch	x	x
Contact contamination	x	
Loose conductive debris		x
Loose contacts		x

result in reliability improvements, the credit for which may be difficult to assign. To gain assurance that the stress screening program is cost-effective, it is essential that the proper data be collected and analyzed. Data other than the screening results are important for use in conjunction with the analysis of screening data. Such data might include: qualification test results, supplier acceptance test results and part receiving inspection results. The screening process must be analyzed as a total process rather than as independent observations of fall-out at each level of assembly. The fall-out at one level of screening is insufficient as a measure of effectiveness. A comparison of fall-out at successive screens provides a basis for reestimating the initial quantity of latent defects, and thereby, screen effectiveness. In addition, using the fall-out data at successive levels of screening provides a high level of visibility as to what is going on in the production process. For example, if part defects are found at upper assembly levels, questions can be posed as to why the defect was not screened out at the part or lower assembly levels. Specific screens can then be devised or existing screens modified to increase the probability that pattern defects found to be escaping lower level screens are detected. Similarly, when pattern assembly defects are found to be occurring, corrective actions such as process or assembly changes can be taken to eliminate the defects from the process." (13)

"The following data are required to be collected at each screening level during production:

      a. Number of assemblies/units exposed to a given screen
      b. Number of assemblies/units passed/failed
      c. Type of defect observed (part, workmanship, design).

"The data analyses to be conducted during the screening program should be directed to establishing if the initial projections of cost-effectiveness of the screening program were reasonably correct and are being maintained. Analysis of the fall-out data should include the identification of "correctable" defects which, if corrective action is taken to eliminate their source/cause, will not recur in subsequent production items. Elimination of correctable defects results in reduced fall out and lower production costs, which may in turn indicate a need to alter the screens. Sufficient elimination of correctable defects may result in no further need for screening. The data analysis required for cost-effective evaluation includes the determination of revised estimates of initial part and assembly defects, revised estimates of screening costs and repair costs at each assembly level." (13)

"Timely, responsive and periodic reporting of the results of stress screening operations to cognizant contractor and government management personnel is essential. The reporting of stress screening results will provide the necessary visibility regarding progress toward achieving the stress screening program objectives. Screening results from early production are extremely important for comparing planned versus actual screening program results. Government personnel should be provided with the necessary information to ensure that planned benefits of the screening program are being achieved in a cost-effective manner. In addition, when contractual changes

may be required to the screening program, Government personnel should require screening result data in order to properly establish revisions to the production contract." (13)

2.3.7 Building to Print

One way to enhance avionic integrity is to identify and characterize. This section reviews, discusses, and identifies avionic production processes and procedures as they are related to the operations and processes involved in the "built to print" of the designed product. Table I-2.3.7-1 shows the approaches and measures for integrity criteria in this stage of the production process.

Having a controlled repeatable production process will ensure integrity. Controlling and correcting the production process will result in manufacturing integrity which is translated into avionic integrity.

Avionics production (Build to Print) consists of the following major tasks:

- Material handling
- Component fabrication
- Panels, covers, and chassis
- Wiring boards
- Integrated circuits
- Hybrids
- Magnetic components
- Harness, cable, and wiring
- Printed wiring
- Board assembly
- Major assembly
- Final assembly.

These tasks convert parts and materials into final assemblies.

Material Handling

Material handling is an important aspect of the manufacturing process. The material handling methods must not introduce new or unknown variables into manufacturing which may or may not be noticed during testing. Material handling, for example, must minimize the probability of damage to electrostatic sensitive components.

"Consideration should be given to the special handling of electrostatic sensitive parts in accordance with DOD-STD-1686 and DOD-HDBK-263". (25) "ESD sensitive parts include microcircuits, discrete semiconductors, thick and thin film resistors, chips, and piezoelectric crystals, depending upon the magnitude and shape of the ESD pulse." (16) "Special handling considerations should be applied to these devices both in the manufacturing environment and

TABLE 1-2.3.7-1. INTEGRITY CRITERIA AND MEASURES DUE TO BUILD TO PRINT

Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
Build-to-Print	Material Handling Component Fabrication Panels/Covers Fabrication Printed Circuit Board Fabrication Integrated Circuits Hybrids Magnetic Interference (EMI) Cables Connectors Assembly: ● Test ● Major ● Miscellaneous Inspection: ● Visual ● Electrical	Reliability Maintainability Manufacturing Quality Quality Assurance Manufacturing Technology Assessment Lifetime (Durability) Supportability Testability Repairability	Material handling electrostatic sensitive parts	DOD-STD-1686, DOD-HDBK-263, fewer damaged parts and less rework
			Following vendor equipment specifications	Tighter process control, fewer damaged parts, and less rework
			Specific instructions for manufacturing steps	Fewer damaged parts and less rework
			Use leadless components	Eliminate lead forming and cutting
			Strict maintenance procedures	Fewer damaged parts and less rework
			QA inspection prior to solder touch-up	Assessment of wave-solder process; fewer damaged parts and less rework
			Strick wave solder process control	Reduced defects
			Testing early in the manufacturing process	Reduce cost to repair
			Automation	Eliminate operator error
			Systematic quality management	Fault prevention

in the shipping/handling environment. ESD damage prevention techniques in the shipping/handling environment include the use of antistatic packing materials and antistatic labels." (18)

Component Fabrication

Component fabrication consists of fabricating the following components:

- Panels, covers, and chassis
- Wiring boards
- Integrated circuits
- Hybrids
- Magnetic components
- Harness, cable, and wiring.

Fabrication of panels, covers, and chassis includes the following operations: sheet metal, preform, and machining.

Whenever possible inspection should be integrated into the fabrication operation with a final goal of tighter process control. Sheet metal operations are performed on metalic sheet stock. These operations include pierce and blank, brake, shear, punch, and hydroform.

Preform operations convert raw materials into finished or semifinished shapes. These operations include plastic molding, casting, extrusion, and powder metallurgy.

Milling, drilling, and turning comprise the machine operations that convert raw materials or preforms into finished shapes.

Fabrication of panels, covers, and chassis also includes the following assembly operations: weld, mechanical, and solder.

Welding joins parts together by thermal fusion of the materials. These operations include arc, laser, electron beam, and torch. Mechanical joins parts together using mechanical methods such as riveting, staking, bonding, crimping, and other standard mechanical fasteners. Solder joins the parts together by thermally bonding another material between the component parts without changing the structure of the parts using the following methods: dip, torch and vacuum brazing, and soldering.

"The use of preforms in the brazing process has happened as a result of the industry turning towards more automated assembly processes. Preforms are a combination of filler metals and flux that have been fabricated to allow:

- Uniform flow of the alloy through the joint area
- Accurate control of the amount of alloy used per joint
- Elimination of the hand-feeding operation

● Faster heating methods
● Minimal rejects.

The use of preforms has dramatically contributed to increased pro-
duction rates and are cost-effective because they eliminate excess filler
metal and excess flux." (18)

During the fabrication of panels, covers, and chassis fasteners are
used. "Four factors should be considered when choosing a fastener for a par-
ticular application: function, reliability, tooling and equipment required,
and installed cost. Generally, self-clinching fasteners take less space and
require fewer assembly operations than caged or anchor nuts, and they have
greater reusability and more holding power than sheet metal screws. They are
used where good pull-out and torque loads are required in sheet metal that is
too thin to provide secure fastening by other methods. In fact, the use of
self-clinching fasteners may allow the designer to specify even thinner
material. Because of their compact design and low profile, they also provide
a neat appearance.

"A need for increased product reliability and performance has
produced a growing demand for self-locking screws and locknuts to prevent
loosening of the joints. Locknuts restrict the nut from backing off the bolt
or stud, thereby causing preload to be lost. This lessens the danger of a
bolted assembly failing during operation. Jam nuts, cotter pins, lock wires
and similar devices also restrict backing off to a degree, but with added
weight, inconvenience, cost, and questionable reliability. Weight savings
achieved by using self-locking fasteners are particularly important in
aircraft." (18)

Printed wiring board is the next component fabrication considered.
Printed wiring board warp is an integrity consideration.

"When laminate enters the PC fabrication process, it is subjected to
chemical, thermal and mechanical shocks. With proper control, none of these
steps need cause the board to warp. If the laminate has not been manufactured
properly, however, some of these processes will bring out warp and twist.

"The primary contributors are solder reflow, drilling, routing,
shearing, and baking for the cure of solder masks, etc. Still, if these
processes are kept within the limits recommended by material and equipment
vendors, no damage should occur.

"In particular, the solder reflow operation should be watched. The
speed of the temperature transition in this process is fast enough that the
difference in temperature between the laminate surface and its center can set
up high shear stresses. Again, following recommended pre-heat temperatures,
conveyor speeds and reflow conditions should preclude damage to the printed
circuit boards." (17)

Many times, but not always, integrated circuits, hybrids, and
magnetic components are procured components for the avionic manufacturer, and
are not fabricated.

Integrated circuit fabrication consists of fabricating integrated circuit wafers including both additive and subtractive operations along with inspection and testing of wafers. The integrated circuits are then packaged and tested.

Hybrid fabrication consists of fabricating substrates, assembling components, packing, and testing. Substrates are either thin film or thick film. The thin film substrates are fabricated using additive or substractive methods. While the thick film substrates are fabricated using a screen printing method.

Magnetic component fabrication consists of shaping wire into selected forms, attaching the shaped wire to a terminal, cover wires with an insulating material, and testing.

No matter what level of sophistication the PWB package achieves, some harness, cable, and wiring fabrication are inevitable during the product manufacturing process. "This requirement may be as simple as joining remote displays, switches, or relays to the controlling board, or as sophisticated as joining peripherals to a CPU for a system. In either case connection requires some kind of wiring." (19)

Cable, harnesses and wiring are interconnect technologies required in the final system integration. Physical production includes manufacturing, and testing operations necessary to convert raw materials into finished cable, harness and wiring components for final system integration. Unique requirements are:

- Specific instructions on tooling for special wire termination
- To-from listing to direct the routing of wire
- Special coding requirements for wire identification
- Operator instructions
- Quality instructions.

Various automated tooling and fixtures are part of the fabrication process. Several processes are required:

- Cutting and identifying the wire, preparing the wire for termination, and terminating it by the use of a robotic system.

- Attaching one end of the wire by soldering, wrapping or insertion processes, then routing the wire along an appropriate path and finally terminating the second end of the wire by any of the above processes.

- Dressing the wires, and installing accessories, and then adding the finishing requirements. Although individual wires applied to backplanes, chassis, or subassemblies will probably not be bundled, they may accept insulating sleeves or other accessories.

Inspection and testing consist of the following activities. Observation for nicks, scratches, abrasions, lumps, irregularities in marking,

appearance, deviations from specifications concerning percent of coverage and angle of braid of a braided shield or jacket, improper length, loose fitting materials or parts, or overtight materials or parts which are obvious to the naked eye with no further measurement, cuts, scrapes, proper installation of terminations of tapes, tubes, tags, gaps in insulation at a termination point, missing or damaged parts.

Testing includes checking of connector keying or harness form or shape on a fixture, checking for material identification such as magnetic response or shield wire, proper parts functioning by manipulation. Testing for continuity, insulation resistance dielectric breakdown, etc. is also needed.

Printed Wiring Board Assembly

After components are fabricated or made available through procurement, the printed wiring boards are assembled. Printed wiring board assembly consists of the following: prepare components, install components, electrical interconnection, testing, and other assembly process as required.

Preprocessing:

Electronic boards often require additional processing prior to component assembly. Preprocessing may be a design requirement, such as riveting a connector to the board, which would be very difficult after parts are assembled and the board is wave soldered. It could also be a process requirement, such as baking to remove moisture prior to wave soldering. Board modifications for engineering changes such as cutting tracks, adding holes and eyelets, etc., are performed when dictated by costs or schedule.

Modification of boards (cuts and jumpers to make them work) should decrease with new CAD tools for design analysis and simulation. Cleaning and baking operations should decrease due to higher quality boards and better inventory control. Board modification and testing will be automated because of circuit complexity (multi-layer and very narrow path widths).

Components often require preprocessing prior to the actual assembly operation. A variety of tasks are performed to make the actual assembly operation easier and faster, or to improve product quality. Typical component preparation functions include lead forming, lead trimming, lead tinning, sleeving leads, and burn-in/programming of components such as PROMs.

"Pretinning of component leads and subsequent age control is important. Component lead tinning is performed just prior to lead form and trim and PWB loading operations in order to keep the pretinned leads as clean and fresh as possible. Component leads received from various manufacturers cannot be depended upon to solder consistently." (20)

New designs will use leadless components which require no forming, trimming, or insulation of leads. At present, pretinning appears to be required, but this, too, may disappear as technology improves.

Parts are "kitted" for assembly based on the process to be used (i.e., manual assembly, machine assisted assembly, or automatic insertion). Kitting is performed after all preprocessing of involved parts and components has been completed. The kit will contain all the parts required for assembly, arranged in the order and type of container or carrier required by the process.

Component Installation:

Components may be automatically inserted to a board by a machine. A person is present to load and unload parts and activate the machine. Parts kitted for this kind of assembly are on tape or in specialized containers.

After components are prepared, the components are installed on the printed wiring boards. Printed wiring boards are located in holding fixtures in preparation for populating with components (a fixture may be either stationary or movable). This operation includes the insertion of both electrical and mechanical parts in holes and surface location on printed wiring boards. The location, orientation, and actual placement of the part may be performed manually, semi-automatically, or automatically. In some cases, electrical interconnections may also be made during the placement operation.

Automated checking of assembly will be added to ensure that specified part is properly installed in correct location. Optical systems are now under development. Tactical and electronic sensing are also possibilities.

Certain types of components may be held in place by bonding them to the board, clinching their leads which extend through the board, or mechanically securing them by some other means.

"Perfectly soldered connections must be resoldered if part, polarity, or location errors are made. To minimize error and maximize efficiency, preprogrammed assembly directors are used to aid the production operator at each board load station. The director is checked out carefully for correct loading and a first piece inspection is performed prior to wave soldering for each lot issued, to assure that control of the board loading process is maintained." (20)

Electrical Interconnection:

Electrical interconnection is the function in which components are joined to printed wiring boards.

An electrical connection may be made manually or hand soldering. Other methods are a combination of automated or semi-automated steps such as wave soldering, vapor phase reflow soldering, stitch welding (fusing two metals together), and wire wrapping (a mechanical connection). Most electrical connections are produced by melting and subsequent cooling of an electrically conducting medium (soldering).

Vapor phase and laser soldering will increase in importance for surface mounted components. Process control will increase in importance as contact areas get smaller, spacing between tracks narrowed, and terminations per component get much larger.

To ensure a correct and reusable electrical connection, continuous attention to the process fluids, solvents, and equipment must be maintained.

As the trend toward denser PWB circuitry continues with ever tighter spacings between conductors and components, the importance of correct assembly and soldering techniques increases dramatically. Excessive solder increases the frequency of bridging problems while the dense circuitry and components push fluxing, soldering, and cleaning technology effectiveness to its limits. And higher density PWB's almost invite some entrapments so decisions must be made on how to either tolerate or control the situations as they arise with appropriate changes in fluxes, cleaning solvents, board layouts and materials.

The production of a reliable electrical pathway between electrical components and circuit boards is a critical step in circuit board assembly operations. The function "perform electrical interconnection" requires certain preparatory steps prior to the operation of making the electrical connections. There are a number of alternative mechanisms for performing the actual connection step. A certain amount of touch-up is required before cleaning can take place.

Wave Solder Electrical Interconnection:

"The results of all prior disciplines to obtain and preserve solder-ability culminate at the wave-solder machine. If solderability has been achieved, success then depends upon the proper execution of process disciplines specific to each PWB and to the wave-solder machine employed. Strict maintenance procedures were developed which require specific daily actions and checks prior to operation of these systems.

"Machine operations are performed only by certified wave-solder specialists who verify by checklist proper machine functions prior to beginning wave-soldering operations. When all checks and settings have been made for a given part number, the first piece is soldered and checked prior to running the lot. To assure ongoing uniform performance of the equipment, daily, weekly, monthly, and annual checks and maintenance actions are performed and verified.

"Quality assurance inspection prior to the performance of any solder touch-up provides an ongoing assessment of wave-solder process performance. This approach facilitates touch-up and reinspection operations and provides specific feedback for cause isolation and correction of repetitive defects, related to board-lead problems or controllable wave-solder process variables.

"Meticulous attention to the control of cleaning, plating, etching, and solder reflow processes is required to produce plated through holes of uniform high quality." (20)

"Except for wave soldering, assembly operations are not inherently harmful. Mechanical stress is sometimes induced when parts are bolted or riveted to the board. Lead trimming can also damage the board if done improperly. The only process that is likely to cause warpage is the wave-solder operation.

"As in reflow, it is important to follow pre-heating procedures carefully and to control the soldering operation closely. The important parameters are exposure time and temperature. Remember, thermal shock is being introduced to one side of the board only. This is strongly conducive to warpage. Also, if the board leaves the solder wave in a warped condition, the hardening of solder on component leads may tend to hold the warp in the board.

"For warpage, this is the most critical time in the entire life of the board. Mechanical stresses acting in many directions cause distortions in the board that are not predictable. The distortions are also not always transient--sometimes they remain in the board after it leaves the wave.

"There is little that can be done at this point to protect the board. Certain definite conditions must be met in order to produce good solder joints. The laminate must be able to withstand these conditions, and again, this means rigid controls must be maintained in laminate manufacture." (17)

Vapor Phase Solder Electrical Interconnection:

"The development of surface-mounted packages has spurred the growth of the vapor phase soldering industry. In-line vapor phase soldering, which we will examine here, is the newest wrinkle in this technology and can best be approached by comparing it to its predecessor, the batch loading vapor phase soldering machine.

"In a typical batch loading machine, circuit parts are loaded onto an elevator basket which is lowered, via chain drive, into a two-zone vapor environment. The primary vapor zone, which supplies the heat necessary for reflow, is a saturated vapor of Fluorinert electronic liquid, made by 3M, St. Paul, MN. Several Fluorinert liquids are available, each with a specific boiling point to create various system operating temperatures. The most frequently used, Fluorinert FC-70, has a nominal boiling point of 215 C (419 F). Established above the primary vapor blanket is a secondary vapor blanket of trichlorotrifluoroethane (R-113), which minimizes the loss of the primary vapor from the system.

"Batch systems offer operating flexibility that makes them useful tools for experimentation and for the establishment of surface-mounting production parameters, as well as for actual production systems. Although they may require more setup time, adjustment, and maintenance than their in-line counterparts, they feature separate controls for the product speed through the vapor, the setting of dwell times, and the travel speed out of the vapor. Having these controls separate enables users to study solder alloys with different reflow temperature profiles, using the same reflow system.

"Although the batch loading systems are useful in many circumstances, high volume production of surface-mounted packages requires a simpler, more linear technique. In-line reflow systems meet this need. Parts are placed onto a conveyor belt either manually or by continuous feeding. They are then transported at a selected, constant speed into a single vapor zone where solder reflow occurs. Reflowed parts dry and cool during transport to the system exit for manual or automatic transfer from the system.

"Vapor phase soldering systems have been effective for use in the surface attachment of discrete chips, leadless chip carriers, both plastic and ceramic compliant leaded chip carriers, small outline packages, and sockets for plug-in packages." (21)

Electrical interconnection also includes such operations as masking, applying hold down fixtures, or securing with temporary measures (such as applying wax) and precleaning the boards. The next step entails the rinsing off of the board, touch-up (remove bridging etc.) and/or correct any missing or damaged parts, and laser inspection of solder joints. The final step includes cleaning to remove residues from the electrical connection operation. Cleaning is necessary to ensure that assembled circuit boards meet electrical conductivity requirements while reducing the likelihood of alien substances attacking electrically conductive surfaces.

Testing:

After electrical interconnection, the printed wiring board assemblies are tested. "There are many methods available for testing printed circuit boards. Implementation choices depend on production levels, the number of different assemblies to be tested, the amount of capital funding available, physical space limitations and a host of other factors. Ultimately, of course, decisions are made based on both tangible and intangible costs.

"The earlier in the PCB manufacturing cycle that a problem is identified, the less expensive it is to repair. Before the introduction of automated testing techniques, many boards ended up on a "bone-pile" simply because the cost to repair far exceeded the cost to scrap. With automatic test equipment, a common rule of thumb is that the cost to repair increases by an order of magnitude with each test step. That is, repair of a problem caught at incoming inspection may cost 50 cents, at board-level test 5 dollars, at system test 50 dollars, and at least 500 dollars to correct the problem in the field.

"Testing performed after the board is built is intended to remove defects introduced during manufacture. First-pass yields decrease rapidly with increasing board complexity and the average number of faults per board increases.

"Once a board has been populated, its manufacturing integrity must be assured. Certainly on large boards the probability that the assembly is correct is small (16 percent on boards of 300 components) and the cost to

correct the problems is a significant part of the overall cost to build the board. Loaded board testing can include any or all of the following:

- Visual inspection
- Shorts and opens
- In-circuit test
- Functional test
- System test.

"Visual inspection will catch gross problems such as missing or reversed components or blobs of solder left from the wave-solder machine. However, the accuracy of this step is largely dependent on factors such as operator attention, time, board component density, and so forth.

"Thorough board testing includes incircuit or functional testing, or both, in addition to a system test. The functional test simulates the function of the board, usually accessing it from the edge fingers, but sometimes through a microprocessor socket or a bed-of-nails fixture to increase visibility into deep and complex logic. An in-circuit tester accesses the board through a bed-of-nails fixture often having more than a thousand nails. Software techniques are used to electrically isolate the individual components so that they can be tested separately. Functional testing has the advantages of speed in the testing of a good board, and it will find performance and design problems which are not identifiable by any other method short of a full system test. A functional tester can usually detect only one fault at a time, whereas all faults of a given type will be identified in-circuit in a single pass, and because fault isolation on an in-circuit tester is to the failing component, a bad board test takes only marginally longer than a good one. For example, a board with four shorts might be tested in five seconds in-circuit. Identification of the same shorts on a functional tester could easily take eight to ten minutes." (22)

"Experience indicates that after a certain level of PWB board complexity is reached, all boards that are manufactured contain at least one fault when they reach the end of the production line. Troubleshooting boards of this nature is complex, and involves more than test.

"There are many different ways to test assembled PWBs. These can best be characterized by three major approaches, called loaded board, in-circuit and functional test. A fourth category, actually a combination of distinct tests, is called combined in-circuit/functional test.

1.) "Loaded board test can examine boards under test for the most common manufacturing defects--solder splash shorts, trace copper residuals (or whiskers) and broken traces. In addition, loaded board test also involves testing some simple components on the board. Test coverage, as this test capability usually is called, varies with each tester, but often includes the ability to test resistors and junctions, and sometimes capacitors.

2.) "The in-circuit approach dictates that each component on the board be tested after the board is completely assembled. The reasoning behind this level of test is that if each component tests good, then the entire board

will function as designed. Modern in-circuit testers employ a technique known as "guarding" which allows them to measure the impedance of devices soldered into a circuit and to ignore the effects of surrounding components. Accuracies within a couple of percent are typical, with higher accuracy available.

"This test is generally performed without applying power to the board, and can be recognized by the unique interface between the board being tested and the test system--called a bed of nails. This interface provides internal visibility by placing contacts on many nodes of the board.

3.) "The functional test approach typically powers up the board to determine if it is functioning properly. This type of test generally is called a Go-No Go test. If the board does not pass, it is examined in a fault isolation procedure that continues to look at the board functionally, rather than examine each individual component on the board." (23)

Miscellaneous Assembly Operations

The final operation to consider for the printed wiring board assembly is miscellaneous assembly which includes conformal coatings.

"Six general base-resin categories of conformal coatings for printed circuit boards seem to be in common use today: acrylics, epoxies, "Parylene" (a Union Carbide patent), silicones, urethanes, and, for convenience's sake, ultraviolet, or UV coatings. Several of the larger manufacturers of coatings offer dozens of types within these general categories, so the total number of coatings is large, to say the least.

"One very large division among coatings falls between those which meet military specifications and those which do not. The standard, MIL-I-4658C, specifies the performance of coatings for the Qualified Products List. Many manufacturers offer both QPL and non-MIL-spec products. The spec covers all the types of coatings listed above. It does not include a separate UV category, however, UV materials generally fall into one of the remaining categories, such as acrylic or urethane." (24)

Major Assembly

Major assembly activity covers all assembly operations in the manufacture of electronic assemblies. It usually begins with the mounting of mechanical and electrical parts such as handles and connectors not previously assembled. A prewired harness or backplane is installed and wires are terminated, dressed, secured and checked for continuity and shorts. It is then loaded with electronic board assemblies. After testing, covers are secured, name plates and decals added, and the finish is touched up as required.

2.3.8 Compliance Tests

Compliance tests are a negotiable item in developing the production contract. As a result most compliance tests are specifically called for in the contract and are specifically documented as to how they are to be performed. Compliance testing while shown at the end of production has activities which go on throughout production. No kit, spares assemblies or systems should be shipped without having first passed through final process controls and compliance tests and checks.

The function of compliance is to ensure that having designed a good product it will do what it is supposed to do and once demonstrated then all other products will be produced the same way. It is a check to be sure the product is not leaving the production facility without full processing. One such compliance activity is called Burn-In where equipment has to operate failure free for a specified number of hours.

The principal benefit of having compliance testing is first to assure the buyer is going to be getting electronic hardware that will perform as needed and desired. Second, to reduce the number of equipment "infant mortalities" in the field where they are costly to repair. Because of the increasing ability to control the process and the benefits of stress testing there is currently some preliminary interest in reducing some of the final testing. Again demonstration of high integrity in the field is the measure for judging. The approaches and measures of integrity criteria are shown in Table I-2.3.8-1.

Administratively high-level management interest in supporting the correct application of the required testings, interest in high integrity in the field and concern for obtaining feedback with corrective action are necessary.

From the process perspective there a number of compliance activities discussed below.

"Tests shall be conducted to verify that environmental and reliability requirements are met. Environments and test objectives shall be combined to the extent practical, consistent with cost and overall objectives. Reliability demonstrations shall be Combined Environmental Reliability Tests (CERTs). Software tests shall be conducted as described in DOD-STD-1679 paragraph 5.8." (12)

Flight tests shall be conducted as a final verification of performance in the operational environment and to verify detail environmental data. These tests shall include flight-line (ground) avionics power on tests to simulate the maintenance environment "Should the flight tests reveal the need for change in the hardware or software, the change would normally be made and validated in the avionics integration support facility as previously done before flight testing. At the completion of the flight test, a functional configuration audit may be performed." (12)

TABLE I-2.3.8-1. INTEGRITY CRITERIA AND MEASURES DUE TO COMPLIANCE TESTS

Activity	Sub-Activity	Integrity Parameter	Criteria	Measure
Compliance Tests	Laboratory Test Reliability Qualification Testing Thermal Management Production Sampling System Effectiveness Tests Testability Demonstration Acceptance Testing Software Acceptance Ground/Flight Tests	Reliability Maintainability Manufacturing Quality Quality Assurance Producibility Lifetime (Durability)	Getting hardware that will perform as needed and desired. Second, reducing number of equipment "infant" mortalities in the field.	Failure free operation during testing for specified number of hours.
			Meeting environmental and reliability requirements.	A. Failure-free operation on contracted tests. B. Software tests conducted per DOD-STD-1679 paragraph 5.8.
			Final verification of performance.	A. Failure-free operation of tests as specified in contract. B. Audit test plan/procedures against official test data (include tests for completeness and accuracy).
			Demonstrate that design specifications have been met on parts, components, and avionic systems.	Conducted in accordance with MIL-STD-8100.
			Reliability qualification.	In accordance with MIL-STD-785, Task 303.
			Verification of thermal capabilities of equipment.	In accordance with MIL-STD-785B, Task 305.
			Changing quality of product once it has been qualified.	Production sampling using contract specific criteria and measurements.
			Ability to test to identify hardness in the system.	Specified in contract.
			Providing an acceptable product.	100 percent failure-free operation (as specified in contract).
			Providing acceptable software.	In compliance with DOD-STD-1679 paragraph 5.10.

"An audit of the test plans/procedures are made and compared against the official test data, including checks for completeness and accuracy. Deficiencies are documented, and completion dates for all discrepancies are established and recorded. An audit of the test report is performed to validate that data accurately and completely describes the test." (12)

"Qualification tests shall be performed on parts, components and avionics systems to demonstrate that design specifications have been met and that associated manufacturing processes are satisfactory. Qualification tests shall be conducted in accordance with MIL-STD-810D to the levels of environmental stresses identified in the system and equipment specification. Combined stresses shall be applied at the highest practical level of assembly and on items of intended production (i.e., manufactured where practicable to production drawings, using production tooling, and inspected and tested to approved procedures using production measuring devices). Design changes made to correct performance deficiencies subsequent to qualification shall be requalified by test(s) equal to the original qualification test(s), if portions of the original test(s) are invalidated. A listing of qualified items shall be maintained by the contractor throughout the program." (9)

"Reliability qualification testing shall be conducted in accordance with MIL-STD-785, Task 303, as part of an overall balanced reliability program. Reliability testing requirements shall delineate the conditions under which malfunctions/incidents are classified either primary, secondary or operator induced. Secondary failures result from another primary failure. All failures are relevant." (9)

"Verification tests shall be combined with other scheduled tests as much as possible and shall be in accordance with MIL-STD-785B, Task 305." (9)

Periodic tests shall be performed on a scheduled basis to verify that avionics integrity is maintained throughout the production phase. The nature of the tests, environmental conditions, and the sampling rate should be compatible with the complexity of the production process and the effectiveness of its controls. If an item is produced on multiple lines or by multiple sources, samples from each shall be selected and tested. If the results of such tests indicate that like items in production are suspect, items of that family will be considered nonconforming material and treated accordingly. Causes of all test failures will be identified and appropriate corrective measures will be taken." (19)

"All deliverable SRUs and LRUs shall be inspected and tested to verify compliance with specification requirements. Each acceptance test shall include a specified period of failure-free operation for 100 percent of all deliverables. Acceptance tests shall also include a failure-free operation period on subsystem or system level deliverables.

"Software acceptance testing shall be in compliance with DOD-STD-1679 paragraph 5.10." (9)

2.3.9 Environmental Survey

The environmental survey development, assessment, and final confirmation is an attempt to quantify more accurately the environmental aspects the full-fledged equipment will experience. The work is performed during production because that is when production prototypes are available and can be used to determine their effects in modifying the environment and the environmental effects on them. The approaches and measures of integrity criteria are shown in Table I-2.3.9-1.

The benefits, of course, lie in being better able to qualify and test the components, assembles and systems for the actual environment (that the product will see) with the resultant reduction in field failures.

Administratively the manager has a challenging effort to motivate the staff to do this work with skill and thoroughness. If environmental estimates came in too low, the equipment could have excessive field failures even through the production, process control and compliance testing were done perfectly. Interest and management support are critical to this task.

In order to properly conduct this task, the avionics system integrator should develop a test program designed to verify initial environmental assumptions made in the system design phase studies. Data to be gathered should include avionics bay vibration, temperature levels, and primary power quality as well as other identified variables that will impact the durability of the product throughout its economic (operational) life.

In addition to considering the environmental stress parameters in the design stage (for planning purposes), there are a number of environmental parameters which are present in the avionic equipment that need to be taken into consideration in the manfacturing and test phases. The findings of the initial environmental assessment report need to be confirmed and any identified changes need to be evaluated in terms of their impact on the final product. Without this assessment confirmation, the durability of the product cannot be properly evaluated, which could result in an increase in failure due to inadequate environmental protection.

"The stresses associated with these parameters may be categorized either as characteristic of the particular aircraft and the specific mission the aircraft is flying, or as a characteristic of the geographic location of the aircraft and equipment location within the aircraft. Since the location factors are independent of specific aircraft or aircraft type, the reliability impact of these stresses will be the same for all aircraft. Those stresses which are a function of the specific aircraft and mission are altitude, temperature, temperature cycling, solar radiation, shock acceleration, and vibration. These will have a varying impact on the reliability of avionics for the different aircraft." (10)

In addition to the above environmental factors, the manufacturer needs to consider the environment experienced during shipping or transfer of systems and subassemblies. There is a developing interest in placing environmental stress monitors with equipment to record the actual shipping and storage environments.

TABLE I-2.3.9-1 Integrity Criteria and Measures Due to Environmental Survey

ACTIVITY	SUB-ACTIVITY	INTEGRITY PARAMETER	CRITERIA	MEASURE
Environmental Survey	Environmental Assessment Report Configuration	Reliability Lifetime (Durability)	Develop as best as is possible within time and funds, an understanding of the actual equipment environment.	A. Subjective--judgement as to adequacy compared to previous equipment in similar situations. B. Compare to actual once flight-testing begins.

The environmental survey development during and after production is an attempt to quantify much more accurately the environmental aspects the full-fledged equipment will experience. It is developed during production because it is then when production prototypes are available and can be used to determine their effects in modifying the environment and the environmental effects on them.

The benefits, of course, lie in being better able to qualify and test the components, assemblies, and systems for the actual environment with the resultant reduction in field failures.

Administratively the manager has a challenging effort ahead to motivate the staff to do this work with skill and thoroughness. If environmental estimates come in too low the equipment could have excessive field failures even though the production, process control, and compliance testing were done perfectly. Interest and management support are critical to this task.

Warranty, service life, and supportability data are required to be collected, evaluated, and maintained during the useable life of the product as follows:

(a) Warranty - The avionics integrator needs to provide a failure-free warranty from the date of acceptance of the avionics by the government (DD-250 signature date).

(b) Service life - The avionic subsystems or equipments (LRUs) need to be tracked while deployed in the field in order to accumulate service life data.

(c) Supportability data - The avionic systems integrator should propose (or use) an existing or demonstrated methodology, as well as a data collection procedure, for arriving at logistics support costs (annualized) for the entire avionics system (as well as the LRU's and SRU's). The avionic system integrator should also be able to relate Logistics Support Costs to Life Cycle Costs including "break-even" points at which time it is no longer economical to maintain the current system.

As part of the above assessment, field failures need to be evaluated for potential system design impact. The avionics system integrator needs to implement a failure reporting system compatible with the systems in place within the USAF. The failures need to be diagnosed in order to determine the failure mechanism and the necessary corrective action. The failure reporting system should include:

a. Reporting of all failures;

b. Establishment of uniform requirements for the system integrator, subcontractor, associate contractors, and the government;

c. Analysis of all failures to identify probable cause and corrective actions (hardware/software);

d. Provisions for the use of independent laboratory or other analysis facilities where organic capability is lacking in-house; and

e. Analysis of failure results to assess design maturity.

The avionics system integrator should implement an automated data system which includes data tapes received from the AFM 66-1 system or similar government data system (i.e., AFTO Form 349, AFTO Form 95, SAC Form 226 or government forms) as well as incorporation of the additional narrative data from paper forms to the automated system. The contractor should also include depot repair/failure analysis data integrated into the same automated system. In addition, the system integrator should establish procedures for identifying, tracking and solving testability problems and other related issues.

When the size of the program warrants, the avionics system integrator needs to establish field diagnostics teams to investigate reported failures occurring during compliance testing and early deployment. The team, made up of selected subcontractors, associate contractors and government personnel, should determine if a failure report must be analyzed further, if adjustments to design or manufacturing are required, or if the report can be closed without extensive analysis.

Furthermore, the avionics system integrator needs to implement a program to gather operational environmental data. The program should utilize as much as possible from the flight loads data gathering program. The same sample aircraft used to gather flight loads data is to be used to gather environmental data. The data to be gathered includes as a minimum: temperature, vibration, and primary power quality in the avionics bays. Multiplex data bus error recording is also recommended in order to facilitate failure diagnosis in digital systems. In addition, the environments for shipping and storage should be characterized for the more sensitive electronic systems.

Once the initial buy has been made it is not infrequent that the buyer will decide to make another purchase. The problems for integrity come from the loss of people skills, loss of motivation, and loss of knowledge of just how the product was produced with high quality. To help reduce the difficulties of restart there is a need to specify those things which will reduce the amount of relearning that will have to go on. Basically, the information which needs to be retained is the documentation developed in the preproduction and production phases which specifies what, how, how come, and typical results of the process controls and testing when they are "working as planned". This activity should not be a difficult task if the documentation activities are done right (with integrity).

More specifically, reprocurement data provided by the avionics system integrator should be complete enough to include piece part control stress screening and process control information. In addition, computer-aided manufacturing techniques should be explicitly stated where used to allow

reprocurement of spares to the same level of integrity as the originally manufactured unit.

Administratively management has to insist on completeness during and at the end of production, and specific money and time need to be earmarked for this activity alone. The activity should start with production.

Process-wise all documentation which is prepared should go through a separate review for completeness right after it is generated. If it is not complete in itself (including utilizing cited references) then the reviewer should have the authority to ask and get an adequate document. Once obtained it can be microfilmed for long term low cost storage. This activity is highly clerical except for the review. The review should be done by technical people independent of the staff chain supplying the work. This provides a more unbiased overview and judgment of completeness. In fact, many times the reviewing technical personl can provide the completeness by asking a few questions whose responses are documented in a memo attached to the document. This activity could effectively be subcontracted with the appropriate type of information protection clauses in the subcontract. It can also be a good activity for retired, part-time quality control, process control or engineering staff with company supported clerical help. Experience in spotting deficiencies in the documentation and the ability to take some corrective actions is key to the success of this activity.

REFERENCES

1. Marone, Victor, "Control Costs by Screening Incoming Electronic Parts", Overview, Spring, 1981, page 14.

2. Capitano, J. L., Gould Defense Systems, "Private Presentation to Battelle", September, 1983.

3. Huber, William J., "Producing Quality People", Overview, Spring, 1981, page 4.

4. Adams, Frank G., "Quality and Productivity - The Case for Motivation", Overview, Spring, 1981, page 7.

5. Johnson, C. H., "An Incentive Approach to Manufacturing Reliable Products", Overview, Spring, 1981, page 11.

6. Goers, M. G., Production Planning...", Overview, Spring, 1981, page 30.

7. Dickman, Thomas J., "Quality Assurance in the Selection and Control of Electrical and Electronic Parts for USAF", Private Communication, no date.

8. Cheshire, Major Lee, and Dickman, Thomas, "Draft Military Standard Avionics Integrity Program (AVIP), Wright-Patterson AFB, Ohio, July 10, 1983.

9. Cheshire, Major Lee, and Dickman, Thomas, "Draft Military Standard Avionics Integrity Program (AVIP), Wright-Patterson AFB, Ohio, January 5, 1984.

10. Edwards, E., Flint, S., and Steinkirchner, J., "Avionic Environmental Factors for MIL-HDBK-217, Rome Air Development Center, AFSC, Griffiss Air Force Base, New York, Final Technical Report #RADC-TR-81-374, January, 1982, pages.

11. Simpson, John, "National Bureau of Standards approach to Quality", Test & Measurement World, Volume 3, Number 12, December, 1983, page 38.

12. Hitt, Ellis F.; Webb, Jeffrey J.; Lucius, Charles E.; Bridgman, Michael S.; and Eldredge, Donald (FAA Technical Center), "Handbook -Volume 1. Validation of Digital Systems in Avionics and Flight Control Applications", U.S. Department of Transportation (FAS), July, 1983.

13. Fiorentino, Eugene, "Draft of ESD 'Environmental Stress Screening'", USAF, Rome Air Develpment Center, May 3, 1982.

14. Keeler, Robert, "Manufacturing Process Control Comes of Age", Electronic Packaging & Production, September, 1983, pages 68-71.

15. "Manufacturing Methods and Tecnology for electronics Computer-Aided Manufacturing - Task 3 Report", Battelle's Columbus Laboratories, U.S. Army Missile Command, MMT Project No. 3801075, January, 1983.

16. MIL-STD-1686, dated 2 May 1980; Electrostatic Discharge Control Program, Forward, page iii.

17. Kear, Fred W., "Board Warp: Causes and Prevention", Circuits Manufacturing, December, 1983, pages 34-36.

18. "Fastening and Joining Technology - A Guide to Productivity", Assembly Engineering, May, 1983, pages 82-91.

19. Assembling Engineering, May, 1938, pages

20. Malone, V. L., "Cost Effective: Wave Soldering: A Mandate for Process Control", Overview/Spring, 1981, pages 22-25.

21. Moy, Peter H., "In-Line Reflow Soldering: Not Just a Passing Vapor Phase", Circuits Manufacturing, September, 1983, pages 32-36.

22. Scheiber, Stephen F., "Configuring an Optimal PCB Test Strategy", Evaluation Engineering, October, 1983, pages 62-72.

23. Maczka, Walter J., "The Changing Role of Electronics Test", Assembly Engineering, December, 1983, pages 12-12.

24. Hastie, Wiliam M., "The Overcoat", Circuits Manufacturing, September 1983, pages 38-47.

25 PMC 31.1 - 1978 - Electromagnetic Compatibility of Process Control Instrumentation.

3.0 CONCLUSIONS/RECOMMENDATIONS

3.1 CONCLUSIONS

Based on the review of the literature and discussions with avionic manufacturers and integrators, government and industry personnel, the following has been determined:

From a systems point of view, there really are no "packages" of measures, defining integrity, that can be universally applied in each of the phases of the development cycle. However, it can be inferred that if the system is developed, tested, and implemented at the component, module, subsystem, and system levels with parts control, derating, stress screening (thermal and random vibration), structured design reviews and other related reliability/maintainability process, integrity will be inherent to the system and target impact of the potential failure rates and failure modes associated with the system development is carried out throughout the development cycle by the use of analytical models and other automated statistical tools as well as rigorous reliability growth and testing methodologies, the system can meet the goals established in the initial system specification.

It is important that the previous tools, criteria, and measures which have been identified in this report be used at the correct points in the development cycle. Furthermore, it is important that the user (the procuring agency) and the system contractor agree on the specific points within the program that data packages, design review or testing sequences/results will be made available.

The contractor's probable contribution to integrity is indicated by the "enthusiasm" with which the contractor embraces the philosophy of providing a reliable/maintainable product that allows the system to be available to perform its intended function when required. Furthermore, if the system requires maintenance actions due to a failure or failures which require removal action, the testability of the system due to built-in test/fault-isolation test should be such that mean down time (MDT) is very short (or the ground based test equipment should be sufficiently capable/flexible to assess the problem rapidly).

In order to properly implement an Avionic's Integrity program within the framework of the proposed MIL-STD-XXX, the Air Force needs to establish a system/equipment development process (in flowchart form) with specific milestones where the system designers, the system manufacturer, and the system integrator will evaluate the emerging product and demonstrate compliance. Examples of the flowchart based development process can be obtained from the field of software engineering where much time and effort have been spent in developing testable and reliable software systems. The process diagram included in the proposed MIL-STD-XXX does not include the necessary checkpoints and compliance demonstrations which are necessary to insure usability.

Manual data collection and documentation methods are inadequate.

Project personnel involved in initial/early phases transfer or quit, often without an information transfer. Later phases are staffed by personnel who do not know what had happened or why design decisions were made unless the documentation is complete and maintained at a very high level of detail.

Feedback occurs primarily when the manufacturer's and system integrator's personnel are in the field. Once operation and maintenance are the responsibility of the USAF, the manufacturer and system integrator traditionally get little or no information feedback, unless specific contractual (or otherwise) arrangements are made prior to fielding the system. The information necessary to properly assess the performance of the system is inherent in the system and/or the test sets if the information is properly handled and feedback is made part of the user's and maintainer's responsibility.

Finally, if integrity is to be built in to the product, it will require that the procuring agency, the designer, the manufacturer and the end user pay attention to people, parts, processes, and design in the context of the environment that the product will encounter throughout its life cycle. Furthermore, based on the currently available information it appears that the initial cost of developing the system with the proper parts and the inclusion of environmental stress screening at all levels (to insure that infant and latent failure are removed prior to fielding of the system) will not add more than 10 to 15 percent of the initial procurement. The "small" increased cost in the front end may well result in "large" savings due to decreased spares and maintenance cost when the system is fielded.

3.2 RECOMMENDATIONS

The material needed to develop and implement effective availability, reliability, testability, and maintainability for the Avionics Integrity program currently exists in many military standards and specifications as well as other government, technical societies, and industry documents. In order to make this information readily available and usable in a systematic manner, it is recommended that the USAF develop an interactive computer-aided avionics integrity guide/data base with an accompanying user handbook which must address software and hardware integrity development, use, and maintenance issues. Within the context of the guide/data base and handbook, system/ equipment/software processes must be established for both hardware and software development cycles at the component, module, subassembly and system level as well as the integration, use, and maintenance. The guide/data base and handbook should address issues, methodologies, tools, parameters, criteria and measures related to integrity in the context of an input/output process with established milestones and goals and feedback mechanisms.

It is recommended that automated data collection techniques be implemented and used for acquiring avionics fault, time of occurrence, and other integrity parameter data from the fielded equipment as well as the subjective evaluation or data obtained from design reviews and other evaluations during the development phase. This "integrity data collection system" should include a computer implemented data base which can be used to analyze the raw data that is automatically collected. This data base information could be available to designers who would make use of this data to improve the design of existing or future avionics systems. Manual data collection methods are dependent upon too many personnel which results in high cost, incomplete or incorrect data, and limited availability of that data which is collected.

A "universal" data base for parts should also be developed for use in parts selection, derating, and substitute parts selection when the previously selected part becomes unavailable. The parts database should contain recommended screening tests and procedures based on part type and potential application environments. Similar information should be available for burn-in. Data collected during screening tests and burn-in should be automatically added to the data base.

The use of validated models and methods such as fault trees and failure modes and effects analysis should be required. Industry believes that MIL-HDBK-217D needs to be updated. The case studies revealed that the primary usefulness of MIL-HDBK-217D is that it is a standard which permits comparison of suppliers estimates of reliability, but the estimates do not agree with "real world data". The designers and manufacturers should also be given more freedom to use failure rate data from their internal data bases assuming that they feel that their data is more representative of "real world" failure rates if MIL-HDBK-217D is not updated.

Computer aided design (CAD) and computer aided engineering (CAE) should be required tools in the development of future systems. Such systems are self-documenting and provide the best source of corporate memory in the case of design personnel leaving the project.

Frequent informal and formal design reviews should be held in order to identify discrepancies as early as possible in the system life cycle. The sooner a discrepancy is identified, the greater the chance of minimizing its impact on system life cycle costs.

Environmental stress tests should be performed at each level beginning with the piece parts and concluding at the assembled system level. These tests are particularly valuable during the development of the prototype SRU and LRU. Each fault identified during the tests should be analyzed and a fix designed, evaluated, implemented, and documented for future reference.

In the case of computers, it is recommended that the USAF procure the computer test equipment from the computer manufacturer and not pay for design and development of a computer test set from another manufacturer. This will result in cost savings and minimize problems associated with fault isolation due to differences in computer test sets.

It is recommended that maximum use be made of CAE and computer aided manufacturing (CAM) in both the pre-production and production phases. This minimizes the variability due to human mistakes in the production process. The production environment should be controlled and production items subjected to a combined environmental-reliability test (CERT). Each fault should be analyzed, a fix implemented, and the item retested to assure that the fault has been eliminated.

The LRU and total system hardware and software should be tested in the system integrator's system integration laboratory (SIL). The USAF organization responsible for the maintenance of the system's software should have a SIL nearly identical to that used by the system integrator once responsibility for maintenance has been transferred to the USAF.* In addition, the Operational Flight Program (OFP) should be directly usable by training simulators, and should be part of the deliverables.

---

* Such a facility can be procured as part of the initial contract award to the system integrator and should be built and used during system integration, and production testing prior to field deployment. Once the system is deployed, the logistics and/or maintenance organization should take possession of the System Integration facility and should use it to properly evaluate problem avionics in the "near-real" environment provided by the facility. Such a facility could be designed/built to automatically collect critical data and provide both a data base and a feedback mechanism for continuous assessment of the avionics system.

3.3 SUMMARY

If the appropriate environmental impact assessments are made, and if the physical stresses that cause failure, in the operational environment, are identified and provided for in the design, integration, and manufacturing phases, then it should be possible to build the product <u>right</u> the first time. Which, in turn, means that the expenditure of money, time, and materials planned for reliability growth testing, need not be budgeted for the next generation of avionic systems, since the inherent reliability of the designed system will be equal to the target reliability specified in the procurement document. The approximately 10 to 20 percent additional money required to obtain the best parts (i.e., additional cost due to parts selection, environmental stress screening, parts derating, etc.) to meet the stresses of the intended operational environment will result in reliability integrity with decreased testing, maintenance, and spares provisioning costs equal to or greater than the initial <u>extra</u> investment in quality "up-front".

VOLUME I
APPENDIX I-A

APPENDICES I-A-1 THROUGH I-A-9 FOR
SECTION 2.1.2

(PRELIMINARY DESIGN AND DETAILED DESIGN PHASES)

APPENDIX I-A

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

APPENDIX I-A-1

I-A-1 Piece Parts Selection

A cost-effective parts program, consisting of the use of properly screened and qualified parts which are adequately derated for their application, is the essence of an effective reliability program and the best assurance of a reliable hardware system. The task of selecting, specifying, assuring proper design application, and, in general, controlling parts used in avionics hardware subsystems/systems requiring extensive engineering effort during design development and procurement is the very nature of the integrity program. It is a multidisciplinary undertaking involving the best efforts of component engineers, reliability engineers, design engineers, project/program managers (including system integrators) and procurement personnel (including packing, shipping and receiving). The total effort includes tasks to:

- Analyze the environment and determine physical stresses on parts
- Determine part criticality and reliability
- Establish approval, qualification and standardization procedures
- Prepare parts specifications
- Procure parts which meet the performance, reliability and cost requirements
- Establish and perform incoming acceptance/rejection tests on parts as they are received
- Establish and perform diagnostic, pathologic tests and procedures on both accepted and rejected parts, to establish "physics of failure" mechanisms for critical parts
- Maintain and update "approved parts lists" and "approved suppliers lists" data bases using current, as well as past, performance.

"A general rule for part selection and control is that military standard parts should be used wherever possible. Standard parts may be defined as those which by virtue of systematic testing programs and a history of successful use in equipment, have demonstrated their ability to consistently function within certain specific electrical, mechanical and environmental limits and, as a result, have become qualified to military (MIL) specifications. MIL specifications which thoroughly delineate a part's substance, form, and operating characteristics, exist (or are in preparation) for practically every known type of electronic part. For example:

- MIL-STD-198, Selection and Use of Capacitors.
- MIL-STD-199, Selection and Use of Resistors.
- MIL-STD-701, List of Standard Semiconductors.
- MIL-STD-1562, List of Standard Microcircuits.

In addition, military qualified parts must have passed standard tests within the associated environments for specific piece parts, for example:

- MIL-STD-202, Test Methods for Electronic Parts.
- MIL-STD-750, Test Methods for Semiconductor Devices.
- MIL-STD-883B, Test Methods for Microelectronic Devices.

"If a standard part is not available, special attention should then be given to selection of the best nonstandard part. This involves evaluation of the proposed part in terms of its reliability, history, design, manufacturing, test methods, potential failure modes, number of alternate sources, and a determination of its cost effectiveness."[2] Special consideration should be given to hybrid parts, especially in terms of the thermal stresses that the part is expected to encounter.

"The selection and control effort associated with the selection of a nonstandard part should include the preparation of procurement specifications which, when completed, reflect a balance between the design requirements, quality assurance, and reliability needs consistent with equipment requirements and vendor capabilities. The specifications should include:

- Lot acceptance testing.
- QA requirements (including incoming inspection).
- Qualification testing as required by application and environmental conditions.
- Process control requirements.

"A well controlled parts program involves establishing a vendor control program, audits of vendor processes, the establishment of source inspection where applicable, and the preparation of associated documentation. The parts control efforts include identification of critical parts from the standpoint of reliability, replacement life, cost, and procurement lead time.

"Planning for critical parts control should include provisions for special handling, identification of critical characteristics to be inspected or measured during incoming inspection, material review procedures, traceability criteria and periodic audits. Detailed documentation should be prepared that describes procedures, tests, test results, and efforts to reduce the degree of criticality of each part.

"Approval of nonstandard parts will be required for most new hardware procurements. Approval necessitates the formal submittal of data. This data must include: (1) statistical test data, (2) analytical data for components that are similar to a standard part, or (3) a combination of statistical and analytical data. (Those parts that require formal statistical test data for qualification should be identified as critical items.)"[2]

To meet the subsystem/system hardware reliability, in terms of piece part reliability, varying degrees of parts screens, burn-in tests and manufacturing process control are available and are documented in the referenced military specifications. Table I-A-1-1 shows four defined parts control levels as they relate to the specifications which govern the types of parts which may be used in designing and building a system. The four parts control levels are:

TABLE I-A-1-1. RELIABILITY/QUALITY CONTROL LEVELS AS A FUNCTION OF PART TYPE

	Reliability/Quality Control Levels			
	A	B	C	D
Part Selection				
Microcircuits	ClassA	Class B, B1, B2	Class C	Commercial
Semiconductors	Jan TXV	Jan TX	Jan	Commercial
Resistors	S	R	M, P	-
Capacitors	T, S	R, P	L, M	-

TABLE I-A-1-2. PARTS SELECTION DECISION MAKING CRITERIA

		Reliability/Quality Level			
		CLASS A	CLASS B	CLASS C	COMMERCIAL
Parts Selection Attributes	Reliability	Highest Reliability	High Reliability	Average Reliability	Lowest Reliability
	Cost	Most Expensive	Generally Most Cost-Effective	Relatively Inexpensive	Most Inexpensive
	Supplier Availability	Limited Supplier Availability	Generally Available	Normally Available	Off-the-Shelf Availability
	Delivery Time	Longest Delivery Time	Normal Delivery Time	Short Delivery Time	Shortest Delivery Time
		Use of Systems That Are:			
	System Application (Criticality)	Safety and Mission Critical	Mission Critical	Relatively Non-Critical	Non-Critical
		Use On Systems Where:			
	System Application (Maintenance)	Maintenance Very Difficult and Costly	Maintenance Relatively Difficult and Expensive	Maintenance is Relatively Easy and Inexpensive	Maintenance is Easy and Inexpensive

<u>Class A parts</u>. These will typically be used on critical systems, i.e., those systems with requirements for near zero unscheduled maintenance and preventive maintenance down-time. These parts have the highest reliability; however, they will generally be associated with the highest cost, longest delivery time, and many times only a single supplier.

<u>Class B parts</u>. These parts will typically be used on those systems or equipments where maintenance is difficult or costly and where life cycle support costs will be a major consideration. These parts have high reliability, moderate cost, normal delivery time, and are generally available from more than one supplier.

<u>Class C parts</u>. These parts will typically be used for those systems which are relatively easy to maintain (low Mean-Time-To-Repair (MTTR)) and are noncritical applications. These parts have average reliability, are relatively inexpensive, have short delivery times, and are normally available from multiple suppliers.

<u>Class D (Commercial Level) parts</u>. These parts will typically be used for those systems or equipments which are easy to maintain, are noncritical and are subjected to a commercial environment. They have the lowest reliability, are inexpensive, and are normally available off-the-shelf.

Table I-A-1-2 presents the decision-making criteria for applying the four defined parts control levels as a function of the parts selection attributes.

The decision-indices in Table I-A-1-2 can be used to conduct reliability/maintainability versus cost tradeoff studies. Once an initial selection of quality level has been chosen, an initial reliability/maintainability assessment can be performed based on parts count (complexity) from the initial design studies assuming that estimates of parts failure rates are available. The resultant analysis can be displayed in a graphical form which shows MTBF as a function of parts count complexity (see Figure I-A-1-1). The data in this figure can be used as an early measure of the system's integrity, which can in turn be used to alter or reinforce the parts quality level selection.

"For example, from Figure I-A-1-1 it can be determined that if an item (subsystem) has 100 parts (integrated circuits, etc.), it can be expected to have an MTBF of between 125 to 1250 hours and a reliability of .955 to .995 over a 5-hour operating period."[3] If those reliability estimates are not sufficient for the specified environment/mission then a 'higher' level of parts quality would have to be chosen in order to increase MTBF."[2]

One of the major questions that the integrity program raises is the balancing of integrity with cost, schedule and performance in the acquisition of avionics equipment. Figure I-A-1-2 presents the general relationships of selected integrity activities (parts selection, derating, reliability growth, production screening and reliability and maintainability programming/surveillance) to acquisition cost. "These cost estimate relationships can be used to
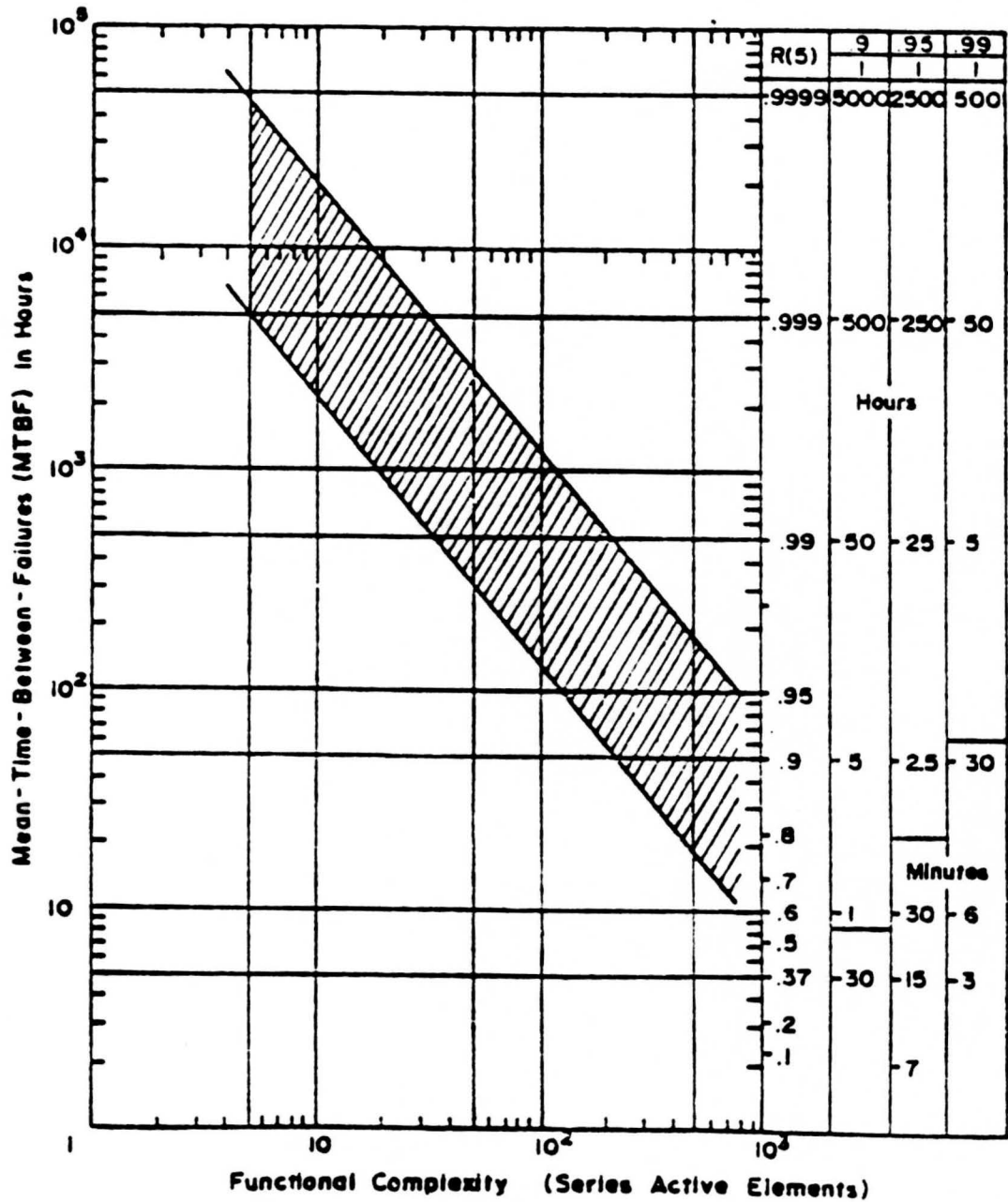
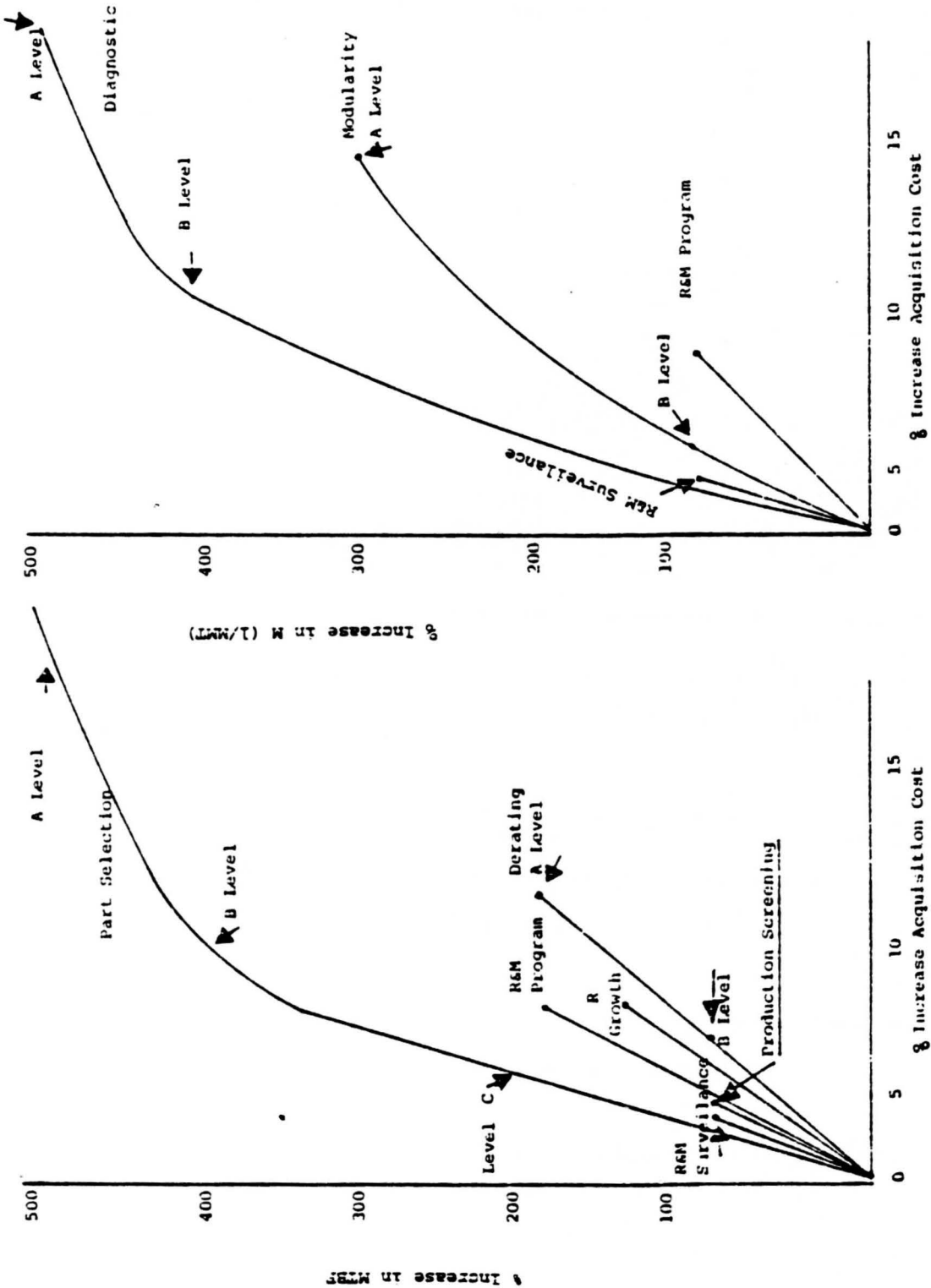FIGURE I-A-1-1. Equipment Reliability Versus Complexity

FIGURE I-A-1-2. R & M Cost Estimating Relationships

produce rough estimates of the scope and cost of reliability and maintainability improvement." "The cost estimate relationships shown in Figure I-A-1-2 provide a basis for determining the reliability and maintainability levels that are most cost-effective and thus incorporated into the hardware procurement specification."[3]

The data in Figure I-A-1-2 sugggest that the cost of providing highly reliable parts control procedures (parts selection, derating, etc., as well as other reliability and maintainability programs) at the earliest stages of the design process will not adversely affect the overall cost of the program (i.e. approximately 10-15% increase in overall cost). However, it can be assumed that if the subsystem/system is developed with quality attributes built-in, due to integrity activities, that the system availability would increase considerably with a corresponding decrease in maintenance actions and a decreased requirement for spares. Correspondingly, if testability is built into the product through the increased use of built-in test and/or fault isolation test, mean time to repair (MTTR), in terms of mean maintenance (MMT) and mean down time (MDT), would decrease due to the ability to diagnose the system quickly. Furthermore, if the subsystem/system was designed and built with modularity as a goal, the ease of repair and isolation at lower levels would result in the failed unit being returned to service quickly, thus increasing availability.

Therefore, the overall cost of providing integrity activities, early in the design activity may be shown to be cost-effective in that a 10-15% initial investment would decrease the overall life cycle cost of procuring and maintaining the system throughout its operational lifetime by (a) making the system available at a higher level (increased MTBF), (b) reducing the spares requirements at the base and depot levels, and (c) by decreasing testability and repairability time requirements through increased modularity and the availability of BIT/FIT to assist in identifying the failure cause.

Table I-A-1-3 summarizes the effect of piece part selection on the various design phase activities and the impact on the various integrity attributes. From this table, it can be seen that piece part selection is important to all design phase activities and will definitely impact the initial cost of the system as well as the support costs after the system is deployed. The available literature appears to indicate that if the "best" parts are procured and used in the system, the initial cost will be higher, but the target MTBF of the system will be met, the various operational environments will have a minimal impact on the availability of the subsystem/system, and the maintenance/logistics costs will be kept to a minimum.

TABLE I-A-1-3. PIECE PART SELEECTION INTEGRITY ATTRIBUTES

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.1. PIECE PART SELECTION	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (7) Partition/Allocate Functions to Hardware/Software (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/Interface Specifications DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Reliability Maintainability Availability Repairability Supportability Life Cycle Cost	MTBF MTTR MDT MTBR MMT	Failure Rate Logistics Costs (Spares Provision) Maintenance Support Costs Time (Available) Test Equipment Complexity

APPENDIX I-A-2

I-A-2 Parts Derating

"All electrical/electronic systems have minimum acceptable reliability requirements, even if not formally specified. The parts used in a system are the most critical items for achieving the required reliability. Experience has shown that most field equipment failures are due to failed parts. Prior to about 1960 control of parts reliability was accomplished by use of part specifications and testing for both the parts and the produced equipment. Part application and derating was usually left to the discretion of the designer. Reliability was usually controlled by levying specific Mean Time To Failure (MTBF) requirements on the equipment. Designers achieve this MTBF by allocating to a maximum allowable failure rate for the individual parts.

"This method results in two major deficiencies in achieving the maximum cost effective reliability. First, testing does not duplicate all operating conditions and therefore does not disclose all possible field failure modes. Second, since MTBF is a function of individual part failure rates, it is often possible to compute an acceptable MTBF even if one or more parts are operating at full rated stress levels. A part operating at the full maximum rating is inherently more unreliable and is depending upon an unknown safety margin, if any, built into the device by the manufacturer. Even if a failure due to overstress does not occur in such a part, the time induced degradation rate is increased. This may account in part for the common occurrence of equipment calculated and tested to a specific MTBF which fails to achieve projected reliability in field usage.

"Recognition of these factors has led to the formalization of derating, for many programs by levying derating requirements on all designs within the program." ... "Part derating is one of the means by which the design engineer can improve the inherent reliability of his design. Derating can be defined as the operation of a part at less severe stresses than those for which it is rated. In practice, derating can be accomplished by either reducing stresses or by increasing the strength of the part. Selecting a part of greater strength is usually the most practical approach. Derating is effective because the failure rate of most parts decreases as the applied stress levels are decreased below the rated value. The reverse is also true, the failure rate increases when a part is subjected to higher stresses and temperature. The failure rate model of most parts is stress and temperature dependent.

"At the present time, there is no recognized Air Force standard devoted exclusively to part derating for all environments. In part, the reason is due to the relative newness of using derating requirements as a reliability tool. Another reason is that the establishment of derating levels is somewhat subjective and derating does not lend itself to supporting a large body of mathematical analysis as does other areas of reliability analysis. Most information relating to specific derating requirements is contained in internal contractor or program documentation and is not released for general publication."[4]

"For many part types there is a range of acceptable derating levels between the minimum derating point and the point of over derating. The optimum derating is normally considered to occur at or below the point of stress where a rapid increase in failure rate occurs for a small increase in stress. Three recommended derating levels are selected on the basis of the criticality of the application.

"● Derating Level I (Maximum Derating):

Equipment whose failure would substantially jeopardize the life of personnel, or seriously jeopardize the operational mission or for which repairs are unfeasible or economically unjustified.

Level I derating is judged to be those stress levels below which further reliability gain is negligible or where further derating will create unacceptably difficult design problems. This is intended for the most critical applications where the associated design difficulty can be justified by the reliability requirement.

"● Derating Level II:

Equipment whose failure would degrade the operational mission or would result in unjustifiable repair costs.

Level II derating is considered to be still in the range where reliability gains are rapid as stress is decreased. However, achieving designs with these reductions in allowed stress, is significantly more difficult than at Level III.

"● Derating Level III:

Equipment of lesser criticality than Levels I or II. Equipment whose failure does not jeopardize the operational mission or which can be quickly and economically repaired.

Level III derating is that stress level reduction which creates minor design difficulties and yet generates the largest incremental reliability gain. The large reliability gain is realized because the effects of stress increase dramatically as the absolute maximum rating is approached."[4]

Table I-A-2-1 provides an example of the application of these three derating levels for junction temperature (microcircuits and semiconductors).

The Federal Aviation Administration has added a subdivision to the above derating levels by taking into consideration the equipment reliability and maintainability level. The three defined reliability and maintainability levels for each derating level are:

"Level A. High reliability is required due to high system criticality and/or due to the fact that unscheduled maintenance actions are very difficult and expensive.

TABLE I-A-2-1   DERATED MAXIMUM JUNCTION TEMPERATURE

Maximum Rated Tj (deg C)	Maximum Allowable Tj (deg C)		
	Level I	Level II	Level III
200	115	140	160
175	100	125	145
150 or lower	Maximum rated minus 65	Maximum rated minus 40	Maximum rated minus 20

Level B. Normal reliability is required due to lower system criticality and relatively easy maintenance.
Level C. Relatively low reliability is required due to low system criticality."[3]

Table I-A-2-2[3] lists maximum stresses relative to the three reliability and maintainability levels, as they relate to both digital and analog equipment design and their various operational environments.

The Navy, in their Navy Power Supply Reliability Design and Manufacturing Guidelines program,[5] defined derating as

"simply the practice of designing equipment using parts whose allowable maximum application stresses are constrained to some percentage of the Absolute Maximum Rating (AMR), thus taking advantage of the lower failure rate which results.

"Absolute maximum ratings on parameters are derived by part manufacturers as guidance for designers, in determining whether their part applications are compatible with anticipated worst-case stress conditions in their equipment. An AMR is usually based on one of the following:

(1) The stress point beyond which device performance parameters are not specified or controlled

(2) The stress limit beyond which permanent degradation of parameters may begin to occur.

"In the latter case, there is usually a safety factor in the vendor's AMR. Absolute maximum ratings usually specified on the individual procurement specification/drawing under "reference

TABLE I-A-2-2. FAA DERATING GUIDELINES

PART TYPE	T_j MAX	Environment I						Environment II						Environment III					
		Digital - 35°C			Analog - 45°C			Digital - 55°C			Analog - 70°C			Digital - 75°C			Analog - 90°C		
		R&M Level			R&M Level			R&M Level			R&M Level			R&M Level			R&M Level		
		A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
Microcircuit	125°C	50	60	70	30	55	70	20	46	70	10	30	55	0	77	50	0	10	35
	150°C	53	62	70	35	67	70	30	55	70	20	45	65	12	86	62	2	30	50
	175°C	55	70	80	50	44	80	31	62	80	28	60	74	22	78	72	12	24	63
Semiconductor	100°C	45	60	70	20	40	60	10	30	52	0	15	35	0	10	28	0	0	10
	125°C	50	60	70	25	50	70	20	47	70	5	37	55	0	28	50	10	10	36
	150°C	50	60	70	30	60	70	27	55	70	15	40	70	12	37	64	0	25	50
	175°C	55	70	80	40	70	80	35	63	80	25	55	80	22	50	77	13	40	45
	200°C	55	70	80	40	70	80	37	65	80	30	55	80	77	52	79	18	45	70
Resistor Fixed Composition		50	65	80	50	65	80	50	65	80	50	63	80	45	58	72	25	33	40
Resistor Fixed Film		60	70	80	60	70	80	60	70	80	45	67	80	47	58	75	25	42	58
Resistor Power W.W.		45	58	72	30	45	58	30	42	55	23	36	48	20	34	45	13	25	38
Resistor Precision W.W.		50	60	70	40	60	70	34	50	70	22	50	70	20	45	70	9	28	30
Capacitor Mica		55	65	75	50	65	70	52	70	78	33	47	60	28	42	57	0	20	40
Capacitor Ceramic I.C.		58	64	70	35	45	70	50	62	72	37	50	63	32	44	60	0	28	44
Capacitor Paper Plastic		50	60	80	42	52	70	44	58	64	44	55	64	43	51	63	24	44	58
Capacitor Glass		52	72	80	34	72	78	33	62	72	44	55	65	36	48	60	20	40	52
Capacitor Ceramic G.P.		55	67	80	43	68	78	30	80	75	48	45	73	30	67	75	8	32	77
Capacitor Tantalum Wet		48	64	78	43	68	75	40	58	72	30	45	63	21	47	30	0	34	57
Capacitor Tantalum Solid		48	64	80	45	60	75	45	60	72	35	53	61	22	50	61	11	42	53

ratings" are derived from vendor's published specifications. The vendor ratings may be verified or modified, as necessary, by test data. These ratings are interpreted as allowable stresses under single occurrence stress conditions, such as encountered during assembly, checkout, screening, or transient operation conditions.

"Operating voltages and power dissipation levels are derated, for particular applications, to insure that the parts will operate at required reliability levels under specified environmental conditions. Voltage and power derating are separate and independent procedures. Voltage derating is done to reduce the possibility of electrical breakdown, whereas power derating is done to maintain the component material below a specified maximum temperature.

"The first step in the process of derating is to establish the operating voltages and the second step is to adjust the power dissipation level. Voltage derating of passive component parts prevents voltage breakdown, flashover, and corona effects at the atmospheric pressure (altitude) to which the parts are exposed. These effects are dependent upon voltage gradients, configuration of terminals, and the nature of the dielectric path. Operating voltages of active parts, such as semiconductors, are dependent on the breakdown characteristics of the semiconductor material.

"After the operating voltages are established, the power dissipation level is determined. The degree of heat transfer from a heat-producing part, and the immediate ambient temperature surrounding the part, will determine the surface temperature or junction temperature at a particular power level. The junction temperature must not exceed 110°C under worst-case conditions."[5]

The Navy, instead of defining derating as a function of environment and reliability/maintainability level, established minimum derating criteria from which they created a table of derating parameters and percent derating as a function of part type (see Table I-A-2-3).[5]

Once the derating criteria are known for a particular application, the designer can perform tradeoff studies and analyses to determine the level of integrity that will be inherent in the final product, and which if the integrity parameters/criteria will be impacted. For example, in the case of a particular component, such as a transistor, the integrity criteria and parameters are analyzed as follows:

A table of calculated values (predicted failure rates) for the three levels of derating (Level I, II and III) are shown in Table I-A-2-4[4] and Figure I-A-2-1.[4] This table demonstrates the change in Mean Time Between Failure (MTBF) that results from applying the different level of derating to both stress and temperature. From this table, it can be seen that if Level I derating is used, the failure rate is .034 x 10^{-6}, whereas for Level II and III derating the predicted failure rates are .277 x 10^{-6} and 6.526 x 10^{-6}, respectively. Therefore, we can conclude that

TABLE I-A-2-3. NAVY PART DERATING CRITERIA

Part Type	Derating Parameter	Derated to % Rating (Or Absolute Value Indicated)
Diodes		
Switching, General Purpose, Rectifier	Current (Surge)	70
	Current (Continuous)	60 (5 amp at 70%)
	Power	50
	Peak Inverse Voltage	65
Zener	Current (Surge)	70
	Current (Continuous)	60
	Power	50
SCR	Current (Surge)	70
	Current (Continuous)	70
	Peak Inverse Voltage	65
All	Junction Temperature	
Microcircuits		
All	Combination of AC and DC loads	Not Recommended
Linear	Current (Continuous)	70
	Current (Surge)	60
	Voltage (Signal)	75
	Voltage (Surge)	80
	Voltage Reverse Junction (Signal)	65
	Voltage Reverse Junction (Surge)	85
	Junction Temperature	
Digital	Supply Voltage	Hold to Manufacturer's Nominal Rating
	Junction Temperature	
	Fanout	80

STRESS RATIO

TEMP	.1	.2	.3	.35	.4	.45	.5	.55	.6	.65	.7	.75	.8	.85	.9	.95	1.0
0	.002	.004	.004	.004	.005	.005	.006	.006	.008	.008	.009	.009	.012	.013	.014	.016	.019
5	.004	.004	.004	.005	.005	.006	.006	.008	.008	.008	.009	.011	.012	.014	.016	.018	.021
10	.004	.004	.004	.005	.005	.006	.008	.008	.008	.009	.011	.012	.013	.015	.017	.020	.023
15	.004	.004	.005	.005	.006	.006	.008	.008	.009	.009	.012	.013	.014	.016	.019	.022	.026
20	.004	.004	.005	.006	.006	.038	.008	.008	.009	.011	.012	.014	.016	.018	.021	.024	.029
25	.004	.004	.005	.006	.008	.008	.008	.009	.011	.012	.013	.015	.017	.020	.023	.028	.034
30	.004	.005	.006	.006	.008	.038	.009	.009	.012	.013	.014	.016	.019	.022	.026	.031	.039
35	.004	.005	.006	.008	.008	.008	.009	.011	.012	.014	.016	.018	.021	.024	.029	.036	.046
40	.004	.005	.008	.008	.008	.009	.011	.012	.013	.015	.017	.020	.023	.028	.034	.042	.053
45	.005	.006	.008	.008	.009	.009	.012	.013	.014	.016	.019	.022	.026	.031	.039	.050	.067
50	.005	.006	.008	.008	.009	.011	.012	.014	.016	.018	.021	.024	.029	.036	.046	.061	.082
55	.005	.008	.009	.009	.011	.012	.013	.015	.017	.020	.023	.028	.034	.042	.055	.074	.104
60	.006	.008	.009	.009	.012	.013	.014	.016	.019	.022	.026	.031	.039	.050	.067	.092	.133
65	.006	.008	.009	.011	.012	.014	.016	.018	.021	.024	.029	.036	.046	.061	.082	.117	.175
70	.008	.008	.011	.012	.013	.015	.017	.020	.023	.028	.034	.042	.055	.074	.104	.152	.236
75	.008	.009	.012	.013	.014	.016	.019	.022	.026	.031	.039	.050	.067	.092	.133	.203	.328
80	.008	.009	.012	.014	.016	.018	.021	.024	.029	.036	.046	.061	.082	.117	.175	.277	.468
85	.008	.011	.013	.015	.017	.020	.023	.028	.034	.042	.055	.074	.104	.152	.236	.390	.692
90	.009	.012	.014	.016	.019	.022	.026	.031	.039	.050	.067	.092	.133	.203	.328	.567	1.058
95	.009	.012	.016	.018	.021	.024	.029	.036	.046	.061	.082	.117	.175	.277	.468	.852	1.684
LEVEL I 100	.011	.013	.017	.020	.023	.028	.034	.042	.055	.074	.104	.152	.236	.390	.692	1.328	2.796
105	.012	.014	.019	.022	.026	.031	.039	.050	.067	.092	.133	.203	.328	.567	1.058	2.158	4.859
110	.012	.016	.021	.024	.029	.036	.046	.061	.082	.117	.175	.277	.468	.852	1.684	3.664	8.878
115	.013	.017	.023	.028	.034	.042	.055	.074	.104	.152	.236	.390	.692	1.328	2.796	6.526	17.120
120	.014	.019	.026	.031	.039	.050	.067	.092	.133	.203	.328	.567	1.058	2.158	4.859	12.242	35.008
LEVEL II 125	.016	.021	.029	.036	.046	.061	.082	.117	.175	.277	.468	.852	1.684	3.664	8.878	24.296	76.273
130	.017	.023	.034	.042	.055	.074	.104	.152	.236	.390	.692	1.328	2.796	6.526	17.120	51.250	
135	.019	.026	.039	.050	.067	.092	.133	.203	.328	.567	1.058	2.158	4.859	12.242	35.008		
140	.021	.029	.046	.061	.082	.117	.175	.277	.468	.852	1.684	3.664	8.878	24.296	76.273		
LEVEL III 145	.023	.034	.055	.074	.104	.152	.236	.390	.692	1.328	2.796	6.526	17.120	51.250			
150	.026	.039	.067	.092	.133	.203	.328	.567	1.058	2.158	4.859	12.242	35.008				
155	.029	.046	.082	.117	.175	.277	.468	.852	1.684	3.664	8.878	24.296	76.273				
160	.034	.055	.104	.152	.236	.390	.692	1.328	2.796	6.526	17.120	51.250					
MAX 165	.039	.067	.133	.203	.328	.567	1.058	2.158	4.859	12.242	35.008						
RATED → 170	.046	.082	.175	.277	.468	.852	1.684	3.664	8.878	24.296	76.273						
TEMP 180	.067	.133	.328	.567	1.058	2.158	4.859	12.242	35.008								
185	.082	.175	.468	.852	1.684	3.664	8.878	24.296	76.273								
190	.104	.236	.692	1.328	2.796	6.526	17.120	51.250									
195	.133	.328	1.058	2.158	4.859	12.242	35.008										
200	.175	.468	1.684	3.664	8.878	24.296	76.273										

NOTES: 1. ALL FAILURE RATES ARE FAILURES PER MILLION HOURS.

2. FAILURE RATES NOT SHOWN ARE GREATER THAN 99.

FIGURE I-A-2-1. NPN Transistor Generic Failure Versus Stress Ratio by Derating Level and Derated Temperature

TABLE I-A-2-4.   GENERIC FAILURE RATE FOR SILICON NPN TRANSISTORS
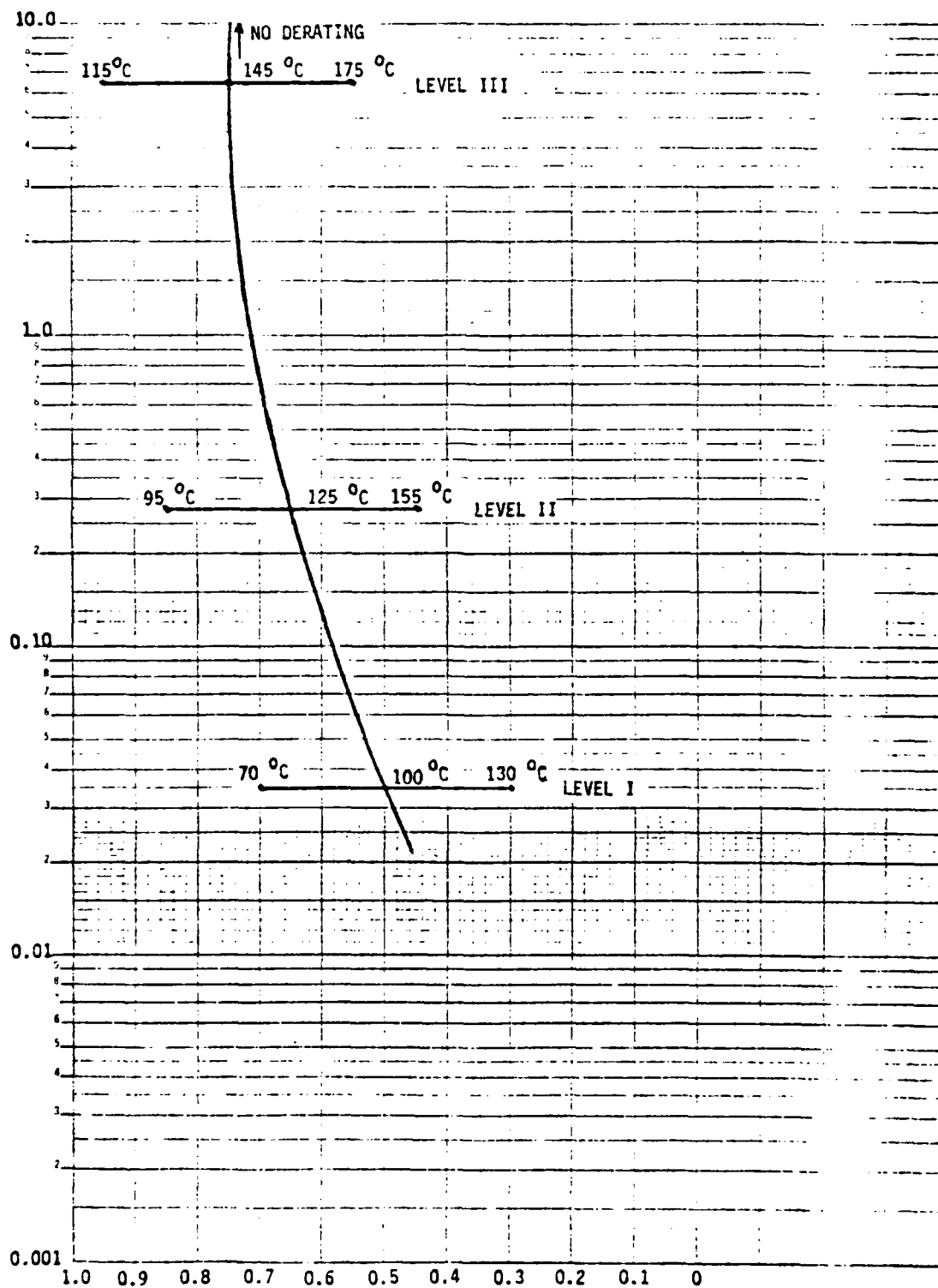
the effects of using parts derating in the design of components/subsystems/systems can be directly measured in terms of MTBF.

In addition to the integrity criteria MTBF, the use of derating will also affect the overall life cycle cost of the component/subsystem/system. If a lesser criticality than that which is actually required is used, the projected increase in failure will result in the necessity to stock a larger number of spares to repair the failed units. On the other hand, if a greater criticality than that which is actually required is used, the cost of producing the desired product will increase unnecessarily due to more difficult design problems associated with the more rigid requirements."

Table I-A-2-5 summarizes the affect of parts derating on the various design phase activities and the impact on the various integrity attributes. From this table it can be seen that parts derating is important to most of the design phase activities, and will impact the design of the subsystem/system depending on the decisions made with respect to the amount of derating and type of applied stress that the subsystem/system can be expected to encounter when deployed.

TABLE I-A-2-5. PARTS DERATING INTEGRITY ATTRIBUTES

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.2. PARTS DERATING	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/ Interface Specifications DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Reliability Availability Life Cycle Cost Supportability Maintainability	MTBF MTBR MDT	Percent Electrical Stress Overload Acquisition Cost Design Constraints/Degree of Difficulty Maintenance Support Costs Operational Environment Reliability Growth

APPENDIX I-A-3

I-A-3 Parts Burn-In

"Most products, whether they be electronic, electromechanical, or mechanical items, will experience a history of reliability which shows a disproportionate amount of failures in the early period of their service. The failure rate is high, but falls off more or less steeply as the product goes into its useful life period, assuming a small and nearly constant failure rate. This is illustrated by the first part of the traditional bath-tub curve. It is the purpose of burn-in to eliminate these early failures to a large extent, before they are experienced in the field. Part failure at any given point in time takes place when the combined effect of the stresses imposed on the part exceeds the part strength at a particular instant. This is the basic reasoning behind the stress-strength model of failure, which is the basis of much recent work on reliability. The reason for the large number of early failures is normally attributed to the fact that variability in production processes, in screening techniques, and in ultimate handling of the parts will introduce weaknesses in some parts and not in others, and it is these weak parts that give rise to the failures witnessed early in the lifetime of the parts.

"A burn-in process, whatever stresses or environment might be imposed, involves time as an important factor. The components, subassemblies, or complete systems are set up in test-rigs and are monitored for failure either continuously or at a predefined time-sequence. The burn-in is stopped, when one is reasonably sure that all the weak items have failed, thus leaving the remaining items in a healthy state of reliability. One of the major problems associated with burn-in is to decide exactly how long the burn-in should continue, balancing appropriately the needs of reliability and the total costs."[6]

The time to failure model used in evaluating burn-in time decisions is based on the assumptions that:

(a) component strength deteriorates with time, and

(b) weak components deteriorate faster than the strong components;

and these assumptions are used in the design and implementation of a cost effective burn-in program. "Deterioration of component strength takes place from the very beginning of the test, and failure occurs when the strength of a component crosses the line of constant stress. The number of components failing per unit of time is computed to give the time-to-failure density function, $f(t)$."[6]

The distribution resulting from the application of burn-in at the component or part level, is bimodal with a small percentage of failures occurring rapidly at lower levels of stress (defined as the freak distribution) and a larger percentage of failures occurring at greater levels of stress (defined

as the same distribution). Figure I-A-3-1 shows the relationship of the two distributions.

The same relationship holds true for both components/parts and sub-assemblies which contain these components/parts. The burn-in tests conducted on the components/parts will yield "freak type" failures, and similarly burn-in test on subassemblies will yield "freak type" failures due to the various production of handling processes during the construction of the product. Both of these failures are due to components that "fail early in life" and constitute "infant mortality failures". The infant mortality failures are primarily made up of gross failures (e.g., cracked chips, open bonds, foreign material contaminants, bad welds, etc.) due to manufacturing or workmanship, and design failures due to inadequate safety margins in board layout or component selection. For these types of failures, the results of using burn-in are almost immediate, in that the greatest number of failure occurs within the first 10-20 hours with a significant dropoff thereafter (see Figure I-A-3-2).

Based on Figures I-A-3-1 and I-A-3-2, if it is decided to use burn-in on selected component types, the components can be stressed optionally by a number of techniques (high temperatures, reverse bias, maximum voltages, etc.), and a large number of temperature and voltage dependent failures can be eliminated in a fairly short time period.

"The percentage of weak components that are built into a system will certainly be reduced if the components have been through a carefully chosen burn-in process. However, an appreciable number of weaknesses will be built into the components during handling and assembly at the equipment manufacturer's plant-weaknesses resulting from, for example, bending and cutting of component leads, overheating during soldering, static electricity, contamination, etc. Also, a number of 'components' are first created during the manufacturing process, for example soldered joints.

"In the case of a system burn-in it is obvious that most components will undergo far from optimal stresses, but on the other hand, weaknesses introduced during system manufacture and weak components created during system manufacture will become apparent."[6]

Therefore, it is necessary to devise a burn-in program that includes not only initial component burn-in, but subassembly burn-in as well. However, both must be accomplished in such a manner that MTTF is determined at a cost-effective point for both components and subassemblies.

"The first steps in burn-in planning may be taken as soon as the design has reached a stage where the general configuration of the product, and the type of components that will go into it, are reasonably well defined. Typically, we might have an electronic circuit diagram, preferably also a preliminary parts list, and an outline of the mechanical design indicating the proposed socket fixtures, transducers, moving parts, etc.; a stage of development, in fact, where the engineering department naturally would perform a reasonably detailed parts-count prediction (MTTF-prediction).
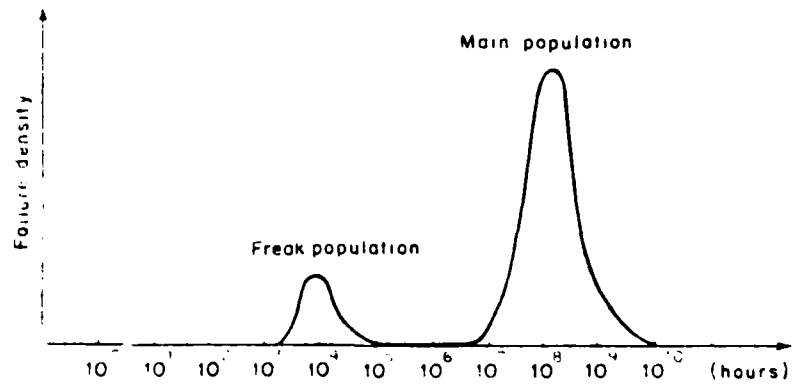
FIGURE I-A-3-1. Freak and Main Population Distributions
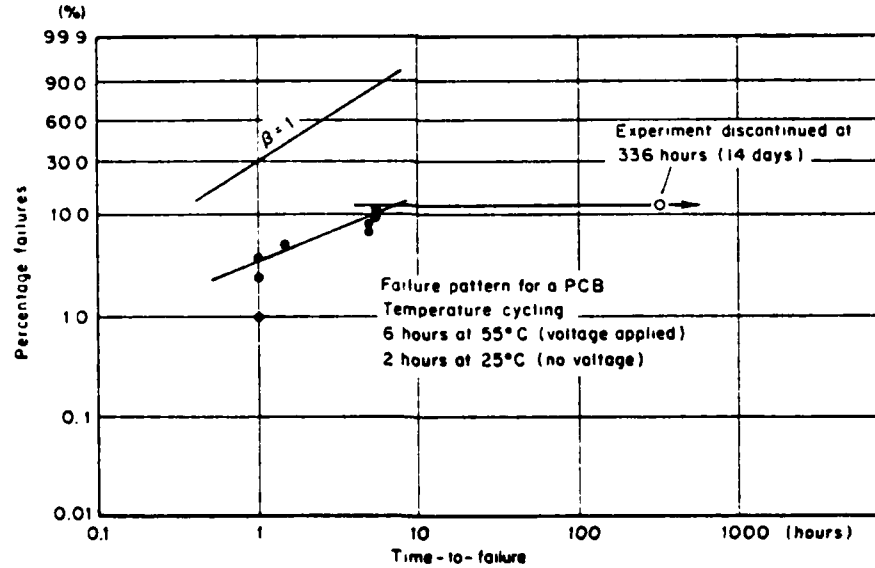
FIGURE I-A-3-2. Failure Pattern of Electronic Control
Equipment on Life Tests

"It is important that at this point in time we seek to gain as much knowledge as possible about the early failure pattern of the product. In other words, we are seeking to predict the early failure distribution, speaking as always of times-to-first-failures. These are six steps in the prediction process. These are listed below:

(1) The critical components or parts must be identified (based on Rate of Change of Stress).

(2) A realistic burn-in environment must be specified (based on greater than the intended actual physical environment).

(3) The time-to-failure parameters of the critical components in the burn-in environment must be found.

(4) For all other components in the design, assume a constant hazard rate. Specific values thereof are found using company data or standard reference tables such as MIL-HDBK-217C (or later editions).

(5) With the above information the early failure pattern of the product may now be computed as a cumulative distribution function.

(6) From the computed curve, drawn on Weibull paper, evaluate the expected percentage weak systems, p_s, and the parameters of the early distribution (i.e., the characteristic lifetime and the Weibull shape parameter).[6]

In conducting the burn-in, based on the above, it must be determined (a) if the burn-in can be optimized with respect to reliability, and (b) if the burn-in can be optimized with respect to cost.

Based on past experience, "... it is known that it is virtually impossible to eliminate all weak components through burn-in, and thus 'guarantee' that the system is in its useful life period, so from this point of view burn-in cannot be optimized. On the other hand, we have also seen that it is possible, using a combination of graphical and analytical methods, to ensure that maybe, say, only one percent of the weak population remains after burn-in is completed. If the system manufacturer has laid down rules for how many weak components may be accepted in those systems that go to the customer, it would be possible using this criteria to determine an optimum burn-in time. If the manufacturer has a stated reliability policy, one will sometimes find that the burn-in time dictated by this policy will be longer than the burn-in time that would be found in a burn-in/cost optimization procedure."[6]

Fortunately, for many systems equipment or components, the burn-in time needed to reach an established reliability goal, and the burn-in time which will be most cost-effective are not far apart (i.e., optimum burn-in will be in the order of a few days, or less).

Since the relationships between the reliability goals and cost-effectiveness goals of conducting burn-in are fairly close, it is easy to develop a burn-in/cost optimizing model with which the integrity of the final product can be evaluated.

The model has two parameters (a) burn-in costs, and (b) field failure related costs. These costs are shown in Table I-A-3-1.

TABLE I-A-3-1.   BURN-IN COSTS AND FIELD FAILURE RELATED COSTS FOR A
BURN-IN COST OPTIMIZING MODEL

Burn-in Costs	Field Failure Related Costs
1. Burn-in Constant Costs (BICC) (Equipment, Installation Testing)	1. Customer Repair Costs (CRC) (Materials, Labor, Time Lost)
2. Burn-in Failure Costs (BIFC) (Handling, Repair, Installation, Testing)	2. Loss of Goodwill (LG) [Constant per failure (to a point)]
3. Burn-in Time Costs (BITC)/D (Per Day Burn-in Time, Production Delay Time, Failure Repair Time).	
4. Diagnostic Analysis Costs. (DAC)	

"If the number of failures during burn-in (FDBI) is estimated (or known) and if the number of failures after burn-in is estimated (or known), the total costs due to burn-in (TCBI) can be predicted (or computed) by:

$$TCBI = BICC + FDBI * BIFC + BITC/D * DAYS + FABI* (CRC + LG).$$

The total costs (TC) due to field failure related costs above (i.e., burn-in is omitted entirely) are

$$TC = FWBI * (CRC + LG).$$

If the cost difference TCBI - TC is calculated and plotted as a function of DAYS burn-in time, the optimum burn-in schedule can be determined (see Figure I-A-3-3)."[6]   Diagnostic Analysis Costs (DAC) need to be added to the TCBI model in order to truly capture all of the related costs.
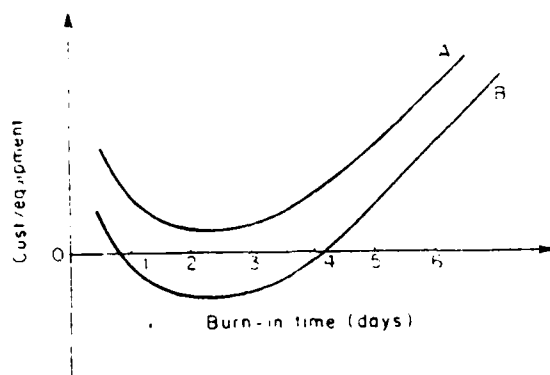
FIGURE I-A-3-3. Typical Curves for TCBI-TC

Using this cost model to optimize the burn-in requirements at the subassembly, subsystem and system levels will result in a product being displayed in the field with very few weak components left to fail and, therefore, by definition a reliable system that will probably meet or exceed the specified MBTF for the system.

Table I-A-3-2 summarizes the effect of burn-in on the various design phase activities and their impact on the various integrity attributes. From this table, it can be seen that burn-in is important to a number of the design phase activities and will impact the cost of the subsystem/system being developed, since it takes money, time, and resources to be completed. However, "the seal test of burn-in efficiency lies in the field failures reported during the first year or two of equipment life. If the burn-in planning and execution has been performed well, then the pattern of field failures should right from the start indicate a constant hazard rate."[6]

TABLE I-A-3-2. BURN-IN INTEGRITY ATTRIBUTES

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.3. BURN-IN	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Reliability Life Cycle Cost Availability Maintainability	MTBF MTTF MTBR MDT MMT	Failure Rate (Early) Failure Rate (Lage) Development Cost Logistics Costs (Spares Provision)

APPENDIX I-A-4

I-A-4 Environmental Stress Screen

Stress screening is a powerful tool for improving the inherent design reliability of the equipment being produced. It can be used at the part, module, subsystem, and system levels with varying degrees of effectiveness, and the cost-effectiveness of this tool can be evaluated by models which can provide quantitative justification for making decisions with respect to the economic costs of the various environmental stress screening alternatives.

Screening to produce highly reliable electronic systems is based on one or more of three general types of screens:

- Environmental (pressure, moisture, temperature)

- Mechanical (acceleration, shock, vibration)

- Electrical (voltage, current, capacitance).

Within the context of one or more specific environments:

- Screening environment

- Reliability test environment

- Field environment.

The development of specific techniques and the application environment needs to be tailored to the end use of the product; and the engineers developing the plan and performing the screening need to be aware that:

1. Not all environments are effective screening environments; the environment which becomes an effective screen is the environment which precipitates the highest percentage of defects, in the shortest time, without degrading the unit being screened; and

2. ...a screen is not a test. Tests imply accept/reject criteria and minimizing failures; screens do not involve accept/reject criteria, and should maximize the number of defects/failures per unit of time and level of stress.

"Screening can be inefficient and costly if the screening stresses are not carefully designed to 'attack' the defective present in the population. Among the risks associated with screening are:

1. Screen will damage good parts.

2. Types of defects will change with time.

3. Screens in use do not attack all defectives present.

4. Screen is being used for defectives no longer in the population.

5. Population of defectives may vary for different production lines.

6. Screen is not based on the reliability level that one is attempting to reach.

These weaknesses suggest that screening should be optimized to produce the most cost-effective screens for various stages of development and production. Theoretically, to optimize screening, one needs a fair estimate of latent failure modes, identification of stresses and indicator parameters useful for detecting these modes, and the selection of the proper sequence of screens. Many times, screening is not optimally designed. Difficulties, for example, arise due to changing characteristics of the product. Thus, screening should be dynamically adjusted during development and production to meet developing program needs."[2]

"Screens are applied as a process to eliminate weak and potentially unacceptable parts through application of stresses prior to assembly (where the costs associated with defective parts becomes multiplicative). Screening should be a cost-effective procedure to provide qualified parts meeting or exceeding reliability targets for assembly into complex electronic equipment. Figure I-A-4-1 illustrates the application of a screen test. It shows temperature/time stress and illustrates, comparatively how reliability screening can improve the part failure rate. It also shows that by applying a higher temperature stress of 125 C instead of 100 C comparable failure rate levels can be achieved in 100 hours instead of 240 hours."[2]

"The best measure of stress screening effectiveness is the quanti- tative improvement in reliability as a result of either introducing a new screen on previously unscreened products or of improving an existing screen. Detailed 'Before/After' reliability data of this type were obtained from nine programs or studies.

"Table I-A-4-1 shows detailed information for several of the nine applications of stress screening. Screening was performed at the unit or system level in seven of the nine cases and at the module (PC board) and com- ponent level for one each case. In all seven cases at unit or system level, the final screening environment had been: increased from no screening at all; or from screening at either a lower stress level; or with a single environ- ment; or both. Also in all seven cases, the final screening included both thermal cycling and vibration (random, sine or both).

"Increased stress screening was shown in all cases (seven cases where field data was available) to result in reduction of field failure rate.
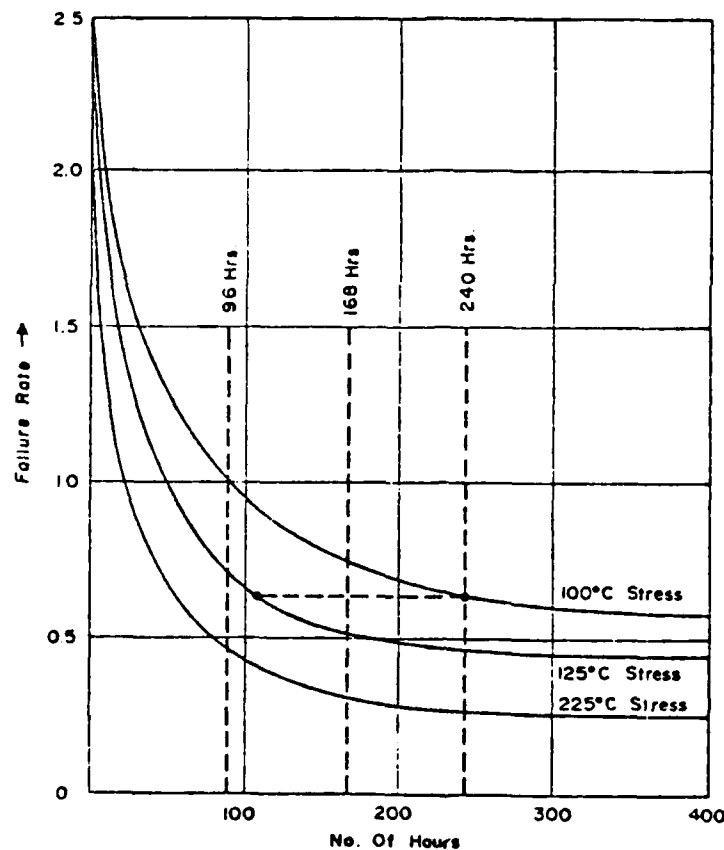
FIGURE I-A-4-1. Reliability Screens

"Percent reduction in field failure rate varied over a wide range. The data show that depending on the application, reduction in failure rate of up to 90 percent is achievable with optimization of stress screening environments with application at the optimum assembly level(s)."[7]

In addition to the data shown in Table I-A-4-1, the study respondents ranked the overall effectiveness of the screens that had been used. Figure I-A-4-2 shows the relative rankings of the various screens. From Figure I-A-4-2 it can be seen that thermal cycling and vibration are perceived to be the most effective screens.

"Much of the data collected during this study contained failure data collected during thermal cycling, where vibration was superimposed for 10 minutes of each hour of operation, thus not providing a direct measurement of the effectiveness of vibration as a screen. For five cases, actual records were supplied as to whether the failures were detected during thermal cycling or vibration. These are summarized in Table I-A-4-2.

TABLE I-4-1. RELIABILITY IMPROVEMENT RESULTING FROM NEW/IMPROVED STRESS ENVIRONMENTAL SCREENING

PROGRAM (APPENDIX B REF)	ASSEMBLY LEVEL OF SCREENING	"BEFORE" (ORIGINAL SCREENING/PROCESSING)	"AFTER" (NEW/IMPROVED SCREEN)	RELIABILITY IMPROVEMENT "AFTER" NEW IMPROVED SCREEN INTRODUCED
Shipboard ECM Receiver A-S3	Unit	300 hrs of burn-in at ambient temperature (25 °C) with power on.	Substituted the following for burn-in: ● 50 hrs temp cycling, -50 to +50 °C power on ● Sine vib 1.4 g PK, 16 hrs	In-house: No measured improvement in MTBF. Field : 20% reduction in field failures.
Tactical Missile (E-M1)	Module Unit	Fixed sine vib 2.2 g rms, 1 axis, 3 min @ guidance unit level of assembly.	PC board level screening added: ● Combinations of different stress levels within the population (literature reference 2)	In-house: 50% reduction in failures at higher assembly levels. Field : 75% reduction in customer receiving inspection failures.
Shipboard Computer A-S2	Component	No screening at any level of assembly.	TX, ER components (diodes, IC's, capacitors, etc) given extra burn-in prior to assembly.	In-house: 66% reduction in in-house failures. Field : 90% reduction in field failures
Communications Receiver A-S1	System	100 hrs burn-in at 50 °C plus 1 g fixed sine vib, 10 min, one time, outside temp chamber.	Added: ● 4 cycles, 0 to 50 °C, power on ● Fixed sine vib at 1 g, 10 min each hr inside temp chamber.	In-house: 70% improvement in demonstrated MTBF. Field : No data.
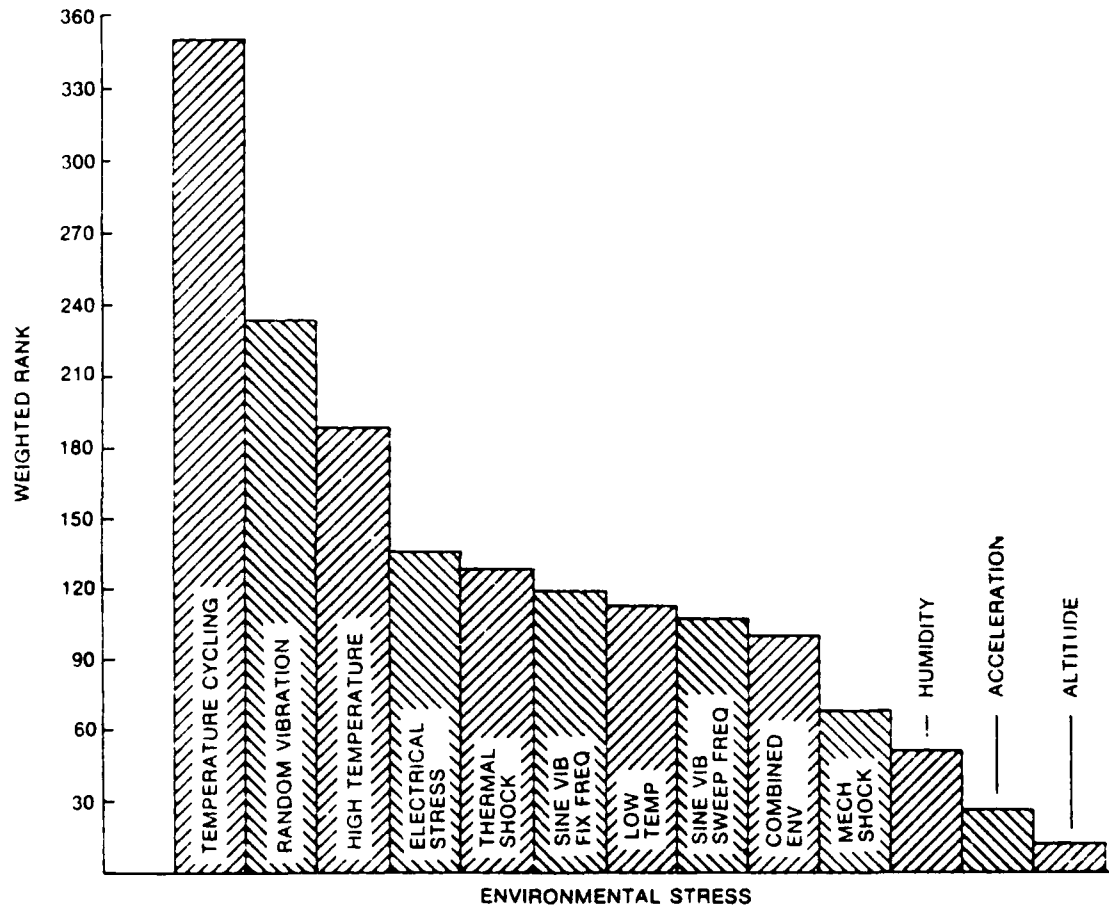
FIGURE I-A-4-2. Effectiveness of Environmental Screens

"The results show that in terms of screening, thermal cycling was generally more effective than vibration for the type of hardware exposed. As shown in Table I-A-4-2 certain equipments are more sensitive to vibration than others. The screening plan must be tailored to the equipment.

"Based on these data, it was concluded that unless an assembly can be determined to contain a predominance of one or the other types of failure mechanisms that can be reasonably quantified, both thermal cycling and vibration will be required for near optimum screening effectiveness.

"Furthermore, based on the above analyses, thermal cycling is the more effective screening environment for electronic hardware. Relative screening effectiveness depends on the mix of potential failure causes inherent in a specific hardware type. On the average, vibration can be expected to screen out from 15 to 25 percent of the precipitated defects. Use of sine vibration will result in the lower limit of screening effectiveness and random the higher. Thermal cycling can be expected on the average to screen out from 75 to 85 percent of the precipitated defects."[7]

Table I-A-4-3 summarizes the effect of environmental stress screening on the various design phase activities and their impact on the various integrity attributes. From this table, it can be seen that environmental stress screening has an impact on most of the design phase activities and will impact the cost of developing the subsystem/system. Environmental stress screening needs to be performed at all levels of system development, however, screening should begin at the piece part and the lowest assembly levels in order to obtain the best results. Piece part selection, part derating, burn-in, and environmental stress screening are all inter-related at the design level where important decisions have to be made within the context of available time, money, and other resources. The design team must make decisions as to how much each will contribute to the overall effort to meet the reliability and availability requirements for the subsystem/system. The development of the proper stress screens is, perhaps, the most challenging part of the environmental stress screen process. The organization responsible for developing the stress screen protocols must take into consideration: the magnitudes of the stresses to be applied; the number of cycles required to stimulate the infant and latent defects; and, the required rates of change ($\pm^{0}C$) required to assure that all of the defects have been removed. The resultant protocols must be developed on the basis of completed environmental assessments, a knowledge of the physical stresses that the parts may be expected to encounter, and the "physics of failure" mechanisms active in the selected parts. If this task is completed properly, then any early failures, in the eventually deployed system, can be traced back to either process or design, but not parts.

TABLE I-A-4-2. DISTRIBUTION OF FAILURES DURING THERMAL CYCLING VERSUS VIBRATION
(UNIT OR SYSTEM LEVEL SCREENING)

PROGRAM (APPENDIX B REF)	SCREENING ENVIRONMENTS AND SEQUENCE	PERCENT OF TOTAL FAILURES EACH SCREENING STEP	PERCENT THERMAL CYCLING FAILURES	PERCENT VIBRATION FAILURES
Electronic Unit (A-A5)	(1) Thermal cycling (2) Vibration, random (3) Thermal burn-in	(1) 77% (2) 10 (3) 13	90% (includes burn-in)	10%
Detecting/Ranging Set (A-A7)	(1) Thermal cycling (2) Vibration, complex random	(1) 42% (2) 58	42	58
Inertial Navigation System (A-A10)	(1) Thermal cycling with sine vibration (2) Vibration, random	(1) 68% (2) 32	68	32
Computer (A-A14)	(1) Thermal cycling (2) Vibration, random (3) Thermal cycling	(1) 60% (2) 10 (3) 30	90	10
Communications Set (A-A4)	(1) Vibration, random (2) Thermal cycling (3) Vibration, random	(1) 1% (2) 97 (3) 2	97	2
	Average Percent Failures		77%	23%

TABLE I-A-4-3. ENVIRONMENTAL STRESS SCREEN INTEGRITY ATTRIBUTES

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.4. ENVIRONMENTAL STRESS SCREEN	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Reliability Life Cycle Cost Availability Maintainability	MTBF MTTF MTBR MDT MMT	Failure Rate (Early) Failure Rate (Lage) Development Cost Logistics Costs (Spares Provision)

APPENDIX I-A-5

I-A-5 Failure Prediction Analysis

Failure prediction analysis techniques need to be used at various stages in the design process in order to assess the impact of failures and failure rates on the reliability of the emerging design. A number of analytical models and methods for analyzing the fault tolerances of digital avionics systems currently exist, however, no single technique has emerged as the standard for conducting failure prediction analysis. The selection of a model or a method for a given application depends on the characteristics of the system to be evaluated, the resources available to the analyst, and the point of the system in its development cycle.

The currently available analytic models and methods are grouped into three classes for discussion of the general capabilities.

1. Failure, Modes, Effects and Criticality Analysis.

2. Fault Trees.

3. Reliability Prediction Models/Techniques.

"Critical to the development of a system that meets its reliability requirements is failure mode analysis. Failure mode analysis involves identifying the items in a system that can fail, defining the modes of failure that are possible for each of these items, and determining the effects of each failure mode on system operation. Failure mode analysis provides a means to identify critical areas for corrective action (e.g., redesign, more reliable parts, etc.) early during development prior to the buildup of prototype hardware and the performance of costly system tests at a time when changes can be implemented easily.

"A complete failure mode analysis is especially required in complex systems where a great degree of interaction is involved. This type of analysis would include:

1. All parts.

2. All possible component failure modes.

3. The probability of failure for each failure mode.

4. The effects on the system or subsystem caused by each failure mode.

5. Each failure mode cause.

6. Possible means of correction or prevention for each failure mode.

"Three techniques are generally used in failure mode analysis. These are listed below and further described in the following paragraphs.

1. Failure mode, effects, and criticality analysis (FMECA) represents a 'bottom-up' analytical approach to failure analysis.

2. Fault tree analysis which represents a 'top-down' analytical approach to failure analysis."[2]

3. Reliability prediction techniques which produce quantitative assessments of the probability of system failure which can be used as an independent check of the other methods.

"1. Failure Mode, Effects, and Criticality Analysis (FMECA). The FMECA approach to failure mode analysis involves systematically identifying and tabulating failure modes at the lowest level of assembly and then determining their effects at higher levels of assembly and ultimately the effect upon the system.

"In its most complete form a failure mode, effects, and criticality analysis is performed to the part level. Failure events are analytically induced into the system and the ultimate effect, frequency of occurrence and severity are then noted. The procedure for conducting a FMECA is described in MIL-STD-1629. Included are six steps as follows:

Step 1. Define the hardware system and its requirements.

Step 2. Establish a logic block diagram (the R prediction block diagram can be used as a starting point for this analysis).

Step 3. Set assumptions and ground rules for performing the analysis.

Step 4. Identify worksheet requirements, including failure modes, effects, failure detection methods, etc.

Step 5. Evaluate criticality of the failure modes.

Step 6. Document the analysis and provide recommendations for design improvement.

"Procedures associated with each step are described in MIL-STD-1629. A FMECA worksheet taken from the procedure outlined in MIL-STD-1629 is presented in Figure I-A-5-1.

FIGURE I-A-5-1. Example of FMECA Worksheet Format

"Based upon the probabilities of lower level failure mode contributions and the failure mode, the probability of system failure modes or system effects can be determined. From these probabilities, and severity factors associated with various system failure modes, critical items, which result in severe system effects due to their failure, can be identified and ranked. These criticality numerics aid in the establishment of field retrofit actions, corrective action priorities, system restoration priorities, and engineering change proposals among others."(2)

"2. Fault Tree Analysis. A fault tree is a graphical representation of the interrelationship between a specific event occurring (a failure) and the ultimate effect it has upon the system. It is an iterative documented process which can be utilized to identify basic system faults, establish their probabilities of occurrence, and ultimately establish their cause and effects. In contrast to the failure mode, effect, and criticality analysis process, a fault tree analysis is a "top-down" approach to failure study. Through analyses of the design, development, test, production, installation, and maintenance of equipment, and the use of fault tree analysis failures throughout the life cycle of an equipment can be studied to determine their cause followed by the formulation of possible corrective action to be implemented to avoid future similar failures. During development, it is considered most effective to be performed during preliminary design and after final design. During preliminary design the analysis is performed to identify failure modes and formulate corrective action suggestions. After final design the analysis is based on detailed design drawings and is performed to show that the system is acceptable with respect to reliability and, if necessary, suggest modifications to the final design.

"The performance of the fault tree analysis methodology, in its most complete form involves: First, the structuring of a detailed logic diagram that depicts the basic faults that can lead to system failure; next, the use of computational techniques to analyze the basic faults and detrmine failure mode probabilities; and finally, a detailed fault matrix which includes all system failure modes, their probabilities of occurrence, and corrective action suggestions that when implemented would eliminate (or minimize) those faults considered critical."(2)

The steps and factors involved in the application of the fault tree failure analysis process are presented in Figure I-A-5-2.

"Fault trees offer several important advantages as shown in Table I-A-5-1. As a top-down documentation procedure, fault trees are useful guides for investigating the possible causes of system or subsystem failures. They are simple to learn. Failure rates are not limited to constant hazard rates since only a probability value is required for each of the lowest level events. Various types of redundancy and dependencies among subsystems can be accomodated if the analyst is clever with conditional probabilities. Several automated fault trees are available to perform the probability computations."(10)
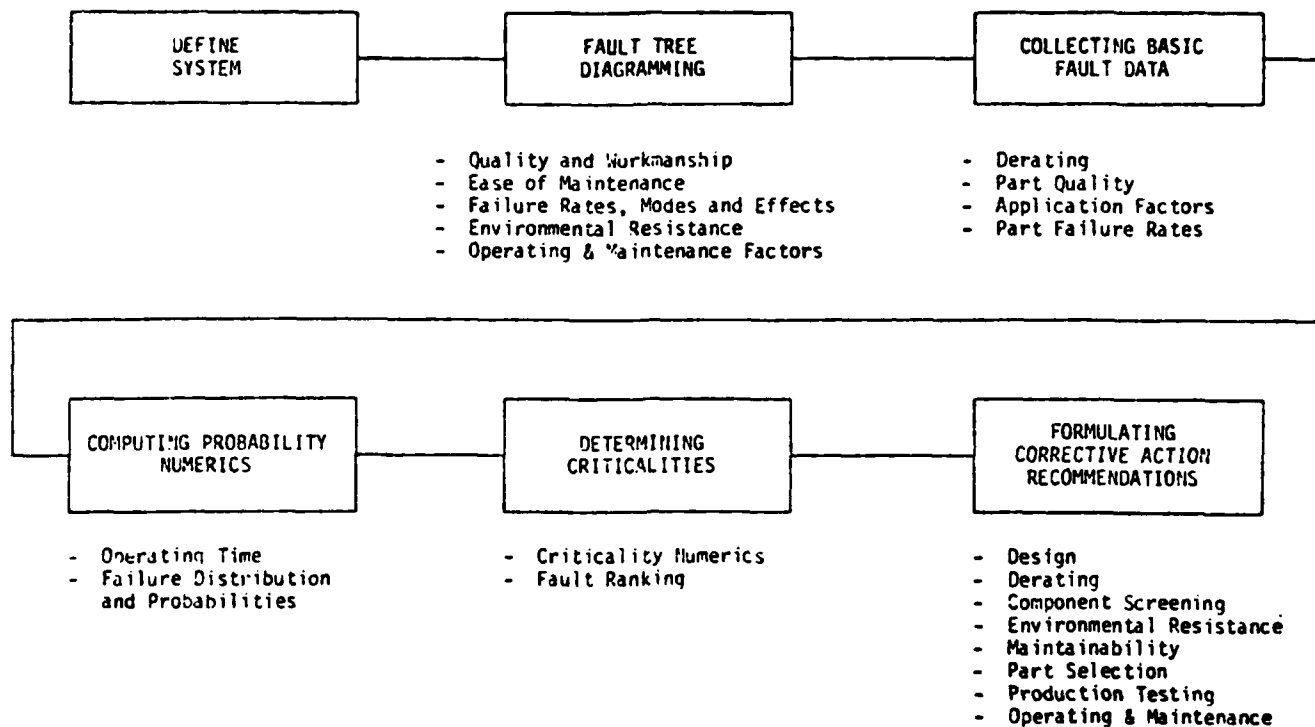
```
┌──────────────┐      ┌──────────────┐      ┌──────────────┐
│   DEFINE     │──────│  FAULT TREE  │──────│COLLECTING BASIC│
│   SYSTEM     │      │  DIAGRAMMING │      │  FAULT DATA    │
└──────────────┘      └──────────────┘      └──────────────┘
```

- Quality and Workmanship
- Ease of Maintenance
- Failure Rates, Modes and Effects
- Environmental Resistance
- Operating & Maintenance Factors

- Derating
- Part Quality
- Application Factors
- Part Failure Rates

```
┌──────────────────┐      ┌──────────────┐      ┌──────────────────┐
│COMPUTING PROBABILITY│   │ DETERMINING  │      │   FORMULATING    │
│     NUMERICS      │     │ CRITICALITIES│      │ CORRECTIVE ACTION│
│                  │      │              │      │ RECOMMENDATIONS  │
└──────────────────┘      └──────────────┘      └──────────────────┘
```

- Operating Time
- Failure Distribution
  and Probabilities

- Criticality Numerics
- Fault Ranking

- Design
- Derating
- Component Screening
- Environmental Resistance
- Maintainability
- Part Selection
- Production Testing
- Operating & Maintenance

**FIGURE I-A-5-2. Steps and Factors Involves in the Application of
Fault Tree Analysis**

TABLE I-A-5-1. FAULT TREE ANALYSIS USES

1. Assure that no system component has any failure mode
    which can result in system failure.

2. Identify which digital modules are involved in
    performing critical functions.

3. Confirm the adequacy of monitoring (i.e., fault
    detection and annunciation in the system).

4. Identify specific software functions required for
    system operation, including fault monitoring
    implemented in software.

5. Provide an alternate means of computing the
    probability of system failure.

3. Reliability Prediction Analysis. Reliability prediction analysis techniques are generally mathematical models which may be manually applied or may be implemented in computer programs. These techniques can be used to evaluate the candidate system prior to the actual development of the hardware and software which implements the proposed design. These techniques analyze the total system and not just a portion of the hardware components of the system.

"Currently available analytic models can be used as tools to assist in the design, engineering development, and certification of digital flight control systems and the specification of the failure mode and overall system reliability. Assessment of system reliability requires assessment of hardware operational faults, design faults, software errors, and man-machine interface faults. Analytic models and methods can provide one aspect of the total equation. The application of these models assure that the software at the module, integration, and system levels have been adequately tested and are free from error.

"In the design phase, models and methods can be used to evaluate the impacts of candidate system architectures and fault-tolerance techniques. Sensitivity analysis can be performed to assess the impacts of variations in levels of redundancy and in effectiveness of coverage. It will usually be sufficient to model coverage as a single parameter for each fault type of interest rather than model the components of coverage."[11]

"The type of reliability prediction model most frequently used in this analysis is a "stage Markov model" such as that presented in Figure I-A-5-3. The "stage Markov model" analyzes stages which include:

Permanent Faults
Transient Faults
Coverage
Detected Stage Failures
Undetected Stage Failures

The "stage Markov model" when completed outputs the data in Table I-A-5-2."[12]

In conducting the failure prediction analysis, it may be desirable to use more than one technique, since no single analytical tool is capable of identifying and predicting all of the fault-tolerant characteristics and failure modes of an emerging design. An approach as outlined in Table I-A-5-3 is one way of assuring that all of the faults and failure modes will be identified and corrected prior to production and field deployment.

EXAMPLE $- l_{34} = 2 \cdot l_p \tau_{34} + 2 \cdot l_T l_{34}$
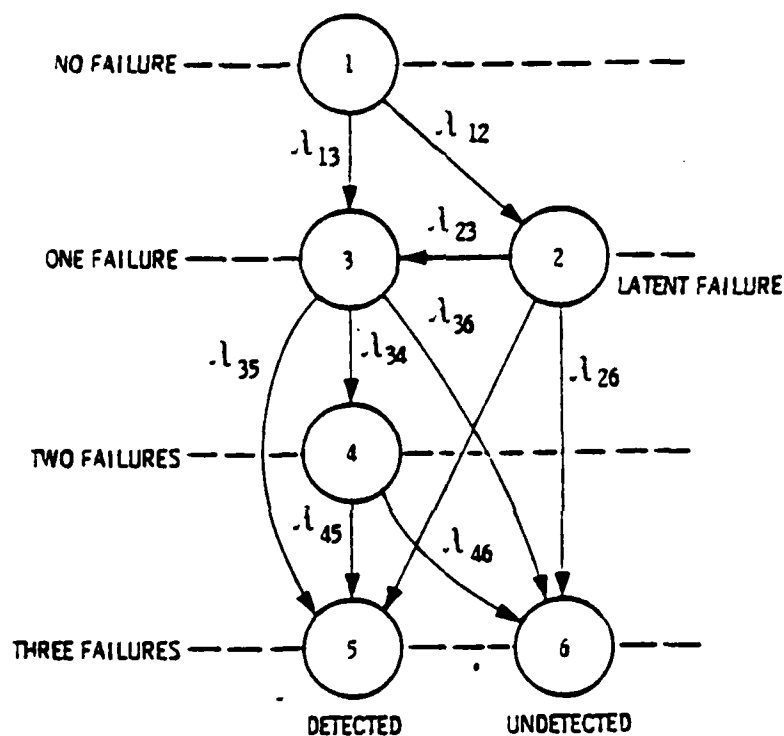
τ - PERMANENT RATE RATIO

l - LEAKAGE

FIGURE I-A-5-3. Example of Stage Markov Model

TABLE I-A-5-2.   STAGE MARKOV MODEL OUTPUTS

I   Functional Readiness Computations

$FR_i(t_1)$ = [PROBABILITY FUNCTIONAL READINESS CONFIGURATION i EXISTS AT TIME t_1]

$PFR(t_1)$ = FUNCTIONAL READINESS = $\sum_{i=1}^{N} FR_i(t_1)$

$PFR(t_1)$ = IS OUTPUT BY CARSRA FOR EACH SPECIFIED TIME t_1

II   System Failure

$FP_i(t_2)$ = PROBABILITY [SYSTEM FAILS BY TIME t_1+t_2 GIVEN FUNCTIONAL READINESS CONFIGURATION i AT TIME t_1]

$PFP(t_2)$ = PROBABILITY [SYSTEM FAILS BY TIME t_1+t_2 GIVEN FUNCTIONALLY READY AT TIME t_1]

$= \sum_{i=1}^{N} FP_i(t_2) \ FR_i(t_1) \ PFR(t_1)$

$PFP(t_2)$ IS OUTPUT BY CARSRA FOR EACH SPECIFIED TIME t_2 AND EACH FUNCTIONAL READINESS TIME t_1

III   Mission Failure

PMF   = PROBABILITY [SYSTEMS DOES NOT MEET ANY FUNCTIONAL READINESS CONFIGURATION OR FAILS AFTER THE FUNCTIONAL READINESS TIME]

PMF   = $[1-PFR(t_1)] + PFR(t_1) \ PFP(t_2)$

TABLE I-A-5-3. ASSURANCE METHOD FUNCTIONS

System Aspect	Assurance Method	
	Primary	Confirmation
Failure Effects		
- Component	Fault Tree Analysis	Fault Insertion
- Digital Module	Fault Tree Analysis, Failure Mode and Effect Analysis	Fault Insertion
- Digital Integrated Circuit	Failure Mode and Effect Analysis	Fault Insertion
- Untractable Cases	Fault Insertion	
Fault Detection/ Annunciation	Fault Tree Analysis	Fault Insertion
Software Function Implementation	Software Test Program	Fault Tree Analysis
No Single-Point Failure Modes	Above, as relevant	Above, as relevant
System Failure Probability	Reliability Prediction Program	Fault Tree Analysis Quantitative Evaluation

Table I-A-5-4 summarizes the effect of failure prediction analysis on the various design phase activities and the impact on the various integrity attributes. From this table, it can be seen that the various tools (fault trees, failure nodes and effects analysis, and reliability prediction models) have an impact on most of the design phase activities and can impact decisions made with respect to design approaches, redundancy requirements and piece part selection and handling. Therefore, it must be stressed that the use of these tools is not only necessary but should be mandatory in order that the "best", most reliable product be developed in the design phase as well as production.

TABLE I-A-5-4. Failure Prediction Analysis Integrity Attributes

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.5. FAILURE PREDICTION ANALYSIS	PRELIMINARY DESIGN PHASE: (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/ Interface Specifications DETAILED DESIGN PHASE: (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Reliability Availability Maintainability Life Cycle Cost	MTBF MTTR MTBR	Cost (Due to Redundancy Requirements) Cost (Due to Component Selection) Life Cycle Cost Failure Rate • Fail Operational • Fail Safe Manpower/Computer Costs to Perform Failure Prediction Analysis Facility Costs (Hot Bench/Pallet for Fault Insertion/Data Collection Maintenance Support Costs

APPENDIX I-A-6

I-A-6 Computer Aided Design

The manual design of printed circuit boards (PCB's) is a tedious and time-consuming occupation that requires meticulous attention to detail. A large board layout may take several months of design effort, and careful checking procedures must be adopted throughout to avoid mistakes. As boards become more complex these problems are compounded. Modern computers, however, have the capacity to store and manipulate vast amounts of data efficiently and quickly; therefore, they are well suited to accept into memory the large amounts of data involved in a board design so that data integrity can be maintained without continued cross-checking with the original circuit.

The different facets of a board design are:

(a) The maintenance of a data base of electronic components and PCB blanks;

(b) The selection of the required components given the data base and their placement on the PCB blank;

(c) The encoding of the circuit for the PCB;

(d) Automatic assignment of correct pad and drill sizes to component terminals/pins;

(e) Link or wire-list determination from the encoded circuit;

(f) Routing of the link list to arrive at the wire layout;

(g) Generation of artwork, production documentation and numerically controlled drill tapes; and

(h) Archiving.

A number of commercially available programs for Computer Aided Design (CAD) are being used by the avionics designers to transform initial design ideas into circuit specifications and diagrams and then to analyze the results using graphics, fault simulation, and automatic test generation. One such system TEGAS-5 (developed by Consat General Integrated Systems, Inc.) provides a full range of digital design requirements from printed circuit boards to full custom integrated circuits through the use of a hierarchical, modular design language.

"The TEGAS-5 program provides a network design language, logic and design verification, worst-case timing analysis, testability analysis, automatic test generation, and fault simulation capabilities.

"Logic and design verification and worst-case-timing analysis are used to study the logical behavior and timing characteristics of digital networks. The modeling of the signal timing propagation is made more complex as the designer progresses through these three design stages. Completed designs can be manufacturered without timing problems.

"Testability analysis processes network topology and interconnect data to provide quantitative analysis of network controllability, observability and testability. Automatic test generation and fault simulation is used to develop tests for the go/no-go quality control tests used during manufacturing. Using the TEGAS-5 program the test engineer is able to make accurate evaluations of the fault coverage provided by the test data and efficiently enhance the data to provide the required coverage."

The TEGAS-5 System has the following capabilities.

"● Applications

The TEGAS-5 program is applicable for the simulation of the vast majority of digital electronic networks, addressing both printed-circuit-board and integrated-circuit design. For custom MOS IC design work, the CGIS TEXSIM design verification system is recommended.

"● TEGAS Design Language (TDL)

TDL is used to describe a network design for simulation. TDL enables the engineer to define networks as entities known as modules, each compiled and stored individually. Modules reside in a user library during development and can be added to a read-only system library upon approval by a system administrator. Modules are created using gate-level devices, functional-level devices, other modules already in a library, or any combination of these. Modules can be nested to 31 levels.

"● Logic Verification

Designers can specify complex waveforms in an arbitrary time frame to be applied to the inputs (and/or internal nodes) at simulation time to verify that the logical implementation of a network is functionally correct. Logic verification typically utilizes unit delay network models to minimize use of computer resources.

"● Design Verification

Switching delay information is included in the network under simulation to identify timing problems within the logically correct design. Delay specifications can be included at the primitive-element level to reflect intrinsic device delays, as well as at primitive-element output pins to reflect loading delays. Separate delay values can be included for rising and falling signal transitions.

"● Worst-Case Timing Analysis

Designers can model minimum and maximum rise and fall delays on primitive-elements and their output pins to verify that the design works within the user-specified range of delay possibilities. Worst-case analysis simulation uses special logic states to represent the regions between the minimum and maximum delay values, which are treated as "unknowns" when they appear on sensitive inputs.

"● Testibility Analysis

COPTR (Controllability, Observability, Predictability, Testability and Reporting) performs analysis of the network with respect to the ease or difficulty of testing at each net for stuck-at-one or stuck-at-zero faults. Reports are available on controllability (net accessability from network input points) and observability (controllability of a network to enable direct detection of net states at network output points). COPTR analysis algorithms process both combinational and sequential logic.

"● Automatic Test Generation

Test pattern generation is based on network topology and information provided by testability analysis. The test generation algorithm is a fourteen valued implementation of the path-sensitization D-algorithm. Utilizing controllability/observability information in this process significantly enhances the effectiveness as well as the efficiency of the generator. Approved test data can be automatically interfaced to commercial testers such as the GENRAD GR16 and the GR1790 series, the Fairchild Sentry series, and others.

"● Fault Simulation

The TEGAS-5 software automatically creates a fault map of stuck-at-one, stuck-at-zero faults on a set of nets specified by the user. A faulted network model for each fault in the map (or a statistical sample) is simulated (in parallel). The program compares simulation output of the good network to that of each faulted network and finds discrepancies at network test points to accomplish fault detection. The STROBE command controls fault detection to the simulation times the user selects. Extensive report options assist in interpreting and using results.

"● Comprehensive drawing management and control

All TEGATE drawings are controlled and maintained on one management directory. The directory maintains revision status, read password, write password, owner password, and last change date. Administrators can control the storage, archival, and release of final drawings through a set of privileged user commands.

"● Two-way interface capabilities to CAD/CAM systems

The TEGATE software automatically produces a complete circuit description after the schematic design has been completed. This data can be transferred to other CAD software such as gate-array and printed circuit board layout systems. After the layout has been completed, the design information can be transferred back to the TEGATE program. Any discrepancy between the circuit as designed and the circuit as implemented is immediately apparent.

"● In-line diagnostics

During design capture, powerful analysis commands prevent ambiguous graphics, electrical shorts, and electrically invalid connections. Other diagnostics include static loading analysis, gate usage analysis, and hierarchy structure validation.

"● Advanced drafting capabilities

The TEGATE drafting capabilities enable schematic designers to produce production-quality drawings much faster than if they used conventional manual techniques. Engineering changes can be rapidly incorporated into work-in-progress, and text management is highly automated. Composition commands aid in partitioning and merging of data between sheets while maintaining electrical integrity."[13]

The use of a CAD tool such as TEGAS-5 for board layout, testing and analysis results in the development of the final designed product at a substantial time and cost savings by the elimination of much of the manual labor required to produce the desired product. The on-line, real time circuit design capability results in savings of money and time through more effective use of existing resources and the ability to automate the transfer of information to other CAD/CAM systems for initial and final production.

Table I-A-6-1 summarizes the effect of using Computer Aided Design during the preliminary design and detailed design phases and the impact on the various integrity attributes.

TABLE I-A-6-1. COMPUTER AIDED DESIGN INTEGRITY ATTRIBUTES

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.6. COMPUTER AIDED DESIGN	PRELIMINARY DESIGN PHASE: (3) Obtain Candidate Subsystem and Components Data (4) Perform Reliability Analysis (5) Perform Maintainability Analysis (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/ Interface Specifications DETAILED DESIGN PHASE: (1) Review Specifications (2) Update Specifications and Drawings (3) Board Design: Placement/Layout/ Thermal Analysis/Power Description (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Reliability Maintainability Availability Repairability Supportability Produceability Manufacturing Quality Life Cycle Costs	MTBF MTTR MTBR MDT MMT	CAD/CAM Interface Costs Life Cycle Costs Development/Testing Costs Data Base Costs Production Costs Time Test Equipment Complexity

APPENDIX I-A-7

I-A-7 Testability

The testability of subsystems/systems can significantly impact the achievement of system performance and cost-effectiveness goals. However, a systematic approach is needed in order to establish and meet the required testability goals and requirements beginning in the earliest program phases through production and development.

Due to the increased complexity and the cost of procurement of modern digial avionics systems, increasing recognition is being given to the correlation between system life cycle costs and the systems' testability characteristics and other integrity parameters.

The testability of a subsystem/system is the inherent ability of an item to undergo valid, functional testing and fault detection/isolation, within the constraints of elapsed time, modularity of the subsystem/system, availability and complexity of support equipment and functional procedures, and within the limitations of manpower, material, and other resources.

"Functional test and condition monitoring are necessary to give assurance and expectation of mission success preparatory to or during operation, and in the course of maintenance or repair. Malfunction detection is necessary to permit consideration of alternative modes of operation and degree of mission success to be expected from use of each alternative mode. Annunciation of the malfunction is a prerequisite to making decisions to conduct maintenance and aids in determining whether or not maintenance will take place with or without system shutdown. Isolation of malfunctions is in turn a prerequisite to effecting repairs or otherwise restoring degraded components to required levels of operating performance."[14]

The above testability activities contribute to the system definition, particularly as requirements in the system specifications. An outgrowth of the testability program definition is the development of specifications for test systems, and a preliminary listing of test equipment and test resource requirements. As systems design detail fills in, the BIT/BITE versus external test allocation is refined. Similarly, qualitative and quantitative testability measures and aims are more closely related to specific functional areas and elements.

"The basic conceptual phase program activities are to conduct system feasibility studies, including identification of alternatives; to establish technical, military, and economic bases for acquisition; and to decide whether or not to pursue the program. It is necessary to consider testability concepts in this phase because of the weight their consideration contributes to the decision process, and to overall program costs. Tables I-A-7-1 and I-A-7-2 summarize the fundamental testability factors that most appropriately should be accounted for during the conceptual phase. The testability relation to other disciplines is indicated in the summary data in Figure I-A-7-1.

TABLE I-A-7-1. TESTABILITY OPPORTUNITIES IN THE CONCEPT PHASE

- Establish Testing Concept
- Outline a Testability Program
- Define functional testing requirements
  - BIT/BITE versus external test equipment
  - Test concepts at hardware identure levels (match existing hardware concept)
  - Test concepts at maintenance levels
    -- Organizational
    -- Intermediate
    -- Depot
- Establish qualitative/quantitative testing goals
  - Thoroughness of condition monitoring
  - Time to detect (isolate)
  - Time to complete functional test
  - Man-hours allocation
  - Cost allocation
  - Management exception trigger level
  - Testability figure of merit/achievement goals/thresholds

TABLE I-A-7-2. TESTABILITY CHARACTERISTICS

• Thoroughness and East of Condition Monitoring - Fault Detection	• Testing is essential to full system effectiveness • Operators need to know the status of system operating modes with full assurance
- Fault Isolation	• Valid, accurate, unambiguous detection and isolation of faults are key to achieving maximum operational availability
- Functional Verification	Functional test is necessary to verify adequacy of performance before and after maintenance

• Constraints of
  - Elapsed Time
  - Simplicity of access
  - Human Resources
  - Test materials
  - All cost-generating elements
	Testability discipline in all aspects has heavy influence on the costs of operating and supporting prime mission equipment systems
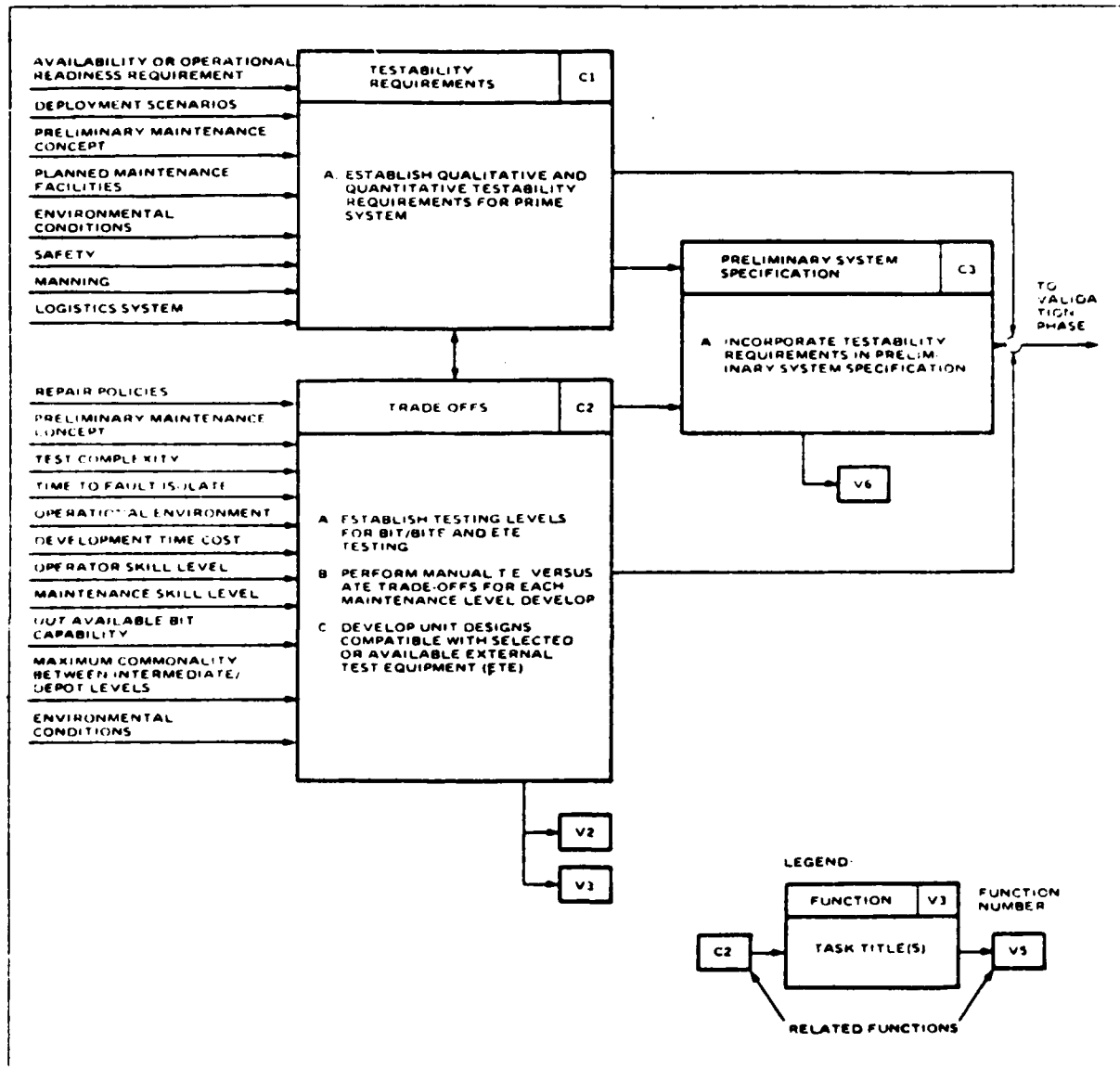
FIGURE I-A-7-1. Conceptual Phase Testability Tasks

"Of great importance at this stage is the interface with system and subsystem design engineers in the applications of complex, difficult-to-test technologies. Detailed planning during this phase ensures availability of the testing capabilities and facilities that will be required in the following development, production, deployment, and operations phases. Opportunities must be exploited at this stage to optimally allocate weight, space, and power to BIT, condition monitoring in general, and maintenance/test functions. In addition to the relationship between reliability and testability allocations, testability aspects must directly consider failure modes and effects and critical items.

"Major interfacings occur between maintainability and testability because of their very close interdependence. In many respects both consider the same elements but in different aspects. Some measures of testability are also measures of maintenance actions, particularly time-to-fault-detect and time-to-fault-isolate. Availability is also directly related to both of these other disciplines because of the need for, and consumption of, system time to perform some actions."(14)

At the earliest stages of the design, the user and the system contractor/integrator need to translate the operational readiness and/or equipment availability requirement into the following testability requirements:

> Maximum allowable time between the occurrence of a failure condition and the reporting of the failure (failure latency) for each mission function;

> Degree of failure tolerance required for each mission function;

> Maximum system downtime due to corrective maintenance actions at the organizational level;

> Testing requirements of backup (standby) equipment and functions in order to accommodate system degraded mode requirements.

The user and the system contractor/integrator then need to refine the testability requirements through an iterative process in which the testability requirements are optimized with respect to other system characteristics, e.g., BIT/ATE utilization, manual/automatic test equipment for system monitoring, and optimizing the mix of BITE, portable testers and maintenance shops to support organizational maintenance. The testability requirements established by this iterative process form the basis for the system specification testability requirements.

The resultant qualitative and quantitative testability requirements should:

- Factor safety considerations into the requirements for failure detection and failure tolerance;

- Be based upon expected numbers and skills of operating and maintenance personnel;

- Be consistent with constraints imposed by the logistic system, including GFE support systems;

- Be consistent with the preliminary maintenance concept, deployment scenarios, environmental conditions and planned maintenance facilities.

The early identification of system characteristics and test subsystem characteristics in terms of subsystem/system testability requirements is essential for the test subsystem to be effective in performance monitoring, fault detection, and fault isolation. Figure I-A-7-2 illustrates these key points.

The user and the system contractor/integrator need to develop an integrated test policy for the system, trading use of manual versus automatic test equipment (ATE) for each maintenance level. They must take into consideration test complexity, repair policy, fault isolation time, functional test time, operational environment, logistic support requirements, development time, skill levels, and all other life cycle acquisition and ownership costs.

Decisions regarding the type of test equipment to be used for system monitoring and maintenance should be based upon repair policies and overall maintenance plans specified in the system specification and the initial hardware functional design. Trade-offs should be made for test requirements at each maintenance level, considering test complexity, time to fault isolate, operational environment, logistic support requirements, development time and cost. The degree of testing automation should be consistent with the planned skill levels of the equipment operators and maintenance personnel.

The resultant trade-off considerations presented in Table I-A-7-3 should be considered with respect to the acquisition of the proper test equipment mix. In addition to the trade-off considerations in Table I-A-7-3, the trade-offs should evaluate the proposed mix of test equipment methodologies for total life cycle costs. This evaluation should include initial price (hardware, software, interfaces, programming requirements, multi-tester complexity, procedures, system turn-around time, system throughput, adaptability to current and future test requirements (ease of modification), and other system specification requirements). The resultant decisions regarding the testability requirements need to be incorporated into the preliminary system specifications along with specifiable goals for test and testability requirements. The testability goals should include, but not be limited to, those which are presented in Table I-A-7-3. Once the testability goals have been established, the subsystem/system designer needs to optimize the preliminary design in light of the system being developed and the test subsystem performance parameters shown in Table I-A-7-3.

In addition to the design criteria presented in Table I-A-7-3 (trade-off considerations, testability goals, and performance parameters), the subsystem/system designer needs to implement the development of the system such that the testability performance measures are accessible and can be
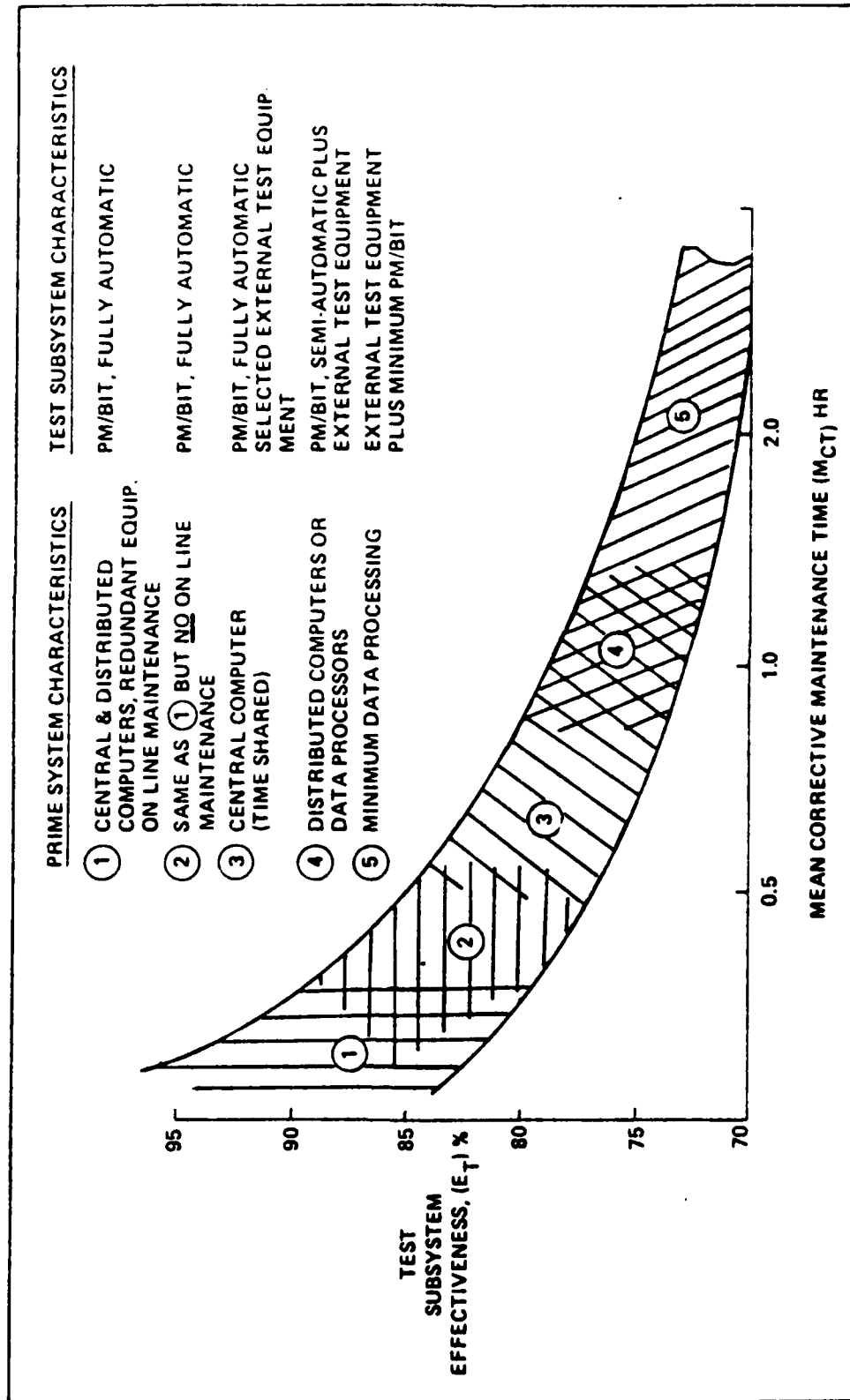
FIGURE I-A-7-2. State-of-the-Art (Circa '75-'80) Prime Systems Versus Test Subsystem Chracteristics

TABLE I-A-7-3. TESTABILITY ATTRIBUTES

1. Trade-off Considerations

- Availability and Maintainability Requirements for the system (LRU or SRU) which will use the test equipment

- Ability of test equipment to meet system (LRU or SRU) test requirements

- Adaptability of test equipment to Design Changes

- Fault isolation and repair time for system (LRU or SRU) under test using test equipment

- Special tester and/or interface requirements for system (LRU or SRU) under test (i.e., microprocessors, RAM, ROM, Hybrid, etc.)

- Utilization rate of specified test equipment (percentage)

- Test equipment programming requirements and cost of software for operational tests

- Test equipment failure rates, fault isolation requirements and time, and repair time

- Cost to buy or develop test equipment

- Development time for specified test equipment

- Number of and skill level of personnel required to support test equipment

- Total life cycle costs for specified test equipment

2. Testability Goals

- Definition of the failure modes specified to be the basis for test design

- Requirement for failure localization to a subsystem/equipment using built-in test

- Requirement for failure isolation to one or more numbers of modules using built-in test

- Requirement for failure localization/isolation times

- Restrictions on built-in test resources in terms of hardware size, weight, power, memory size, and available time

- Requirements for limiting false alarm rate

- Requirement for status monitoring

- Requirement for built-in test hardware reliability

- Requirement for failure detection using passive monitoring only

- Requirement for failure detection using built-in test hardware

- Requirement for failure detection using ground test equipment (Automatic test equipment at Base/Depot level)

3. Performance Parameters

- Availability, operational demand and criticality of subsystem/system to be tested

- Mission duration/operational modes requirements

- Mission reliability requirements

- Built-in test reliability requirements

- Maximum turnaround time due to maintenance action:
  - Expected mean downtime
  - Expected mean logistics/administrative delay time
  - Expected mean corrective maintenance time
  - Expected test equipment effectiveness

- Expected percentage of false alarms (i.e., no defect removal due to "can not duplicate" (CND) or "re-test okay" (RTOK) condition)

- Expected availability/usage of test equipment

4. Performance Measures

- Percent of faults detection:
  - (1) Percent of all faults and out-of-tolerance conditions automatically detected by Built-in Test/Automatic Test Equipment
  - (2) Percent of all faults and out-of-tolerance conditions detectable by Built-in Test/Automatic Test

- Percent of false alarms:
  - (1) Rate at which false indications occur (per 10^6 hours)
  - (2) Percent of indicated failures caused by actual failures
  - (3) Percent of Built-in Test/Automatic Test Equipment indicated failures caused by actual failures
  - (4) Percent of Built-in Test/Automatic Test Equipment fault isolations to the wrong SRU or LRU
  - (5) Percent of erroneous Bit indications

- Mean fault detection time:
  - (1) Time to indicate a fault once it has occurred
  - (2) Time to detect a fault once it has occurred
  - (3) Time to verify that a failure has occurred or has been repaired

- Test thoroughness:
  - (1) Percent of all equipment functions tested

- Fault isolation resolution:
  - (1) Isolation of P_1 percent of the failures to X_1 units under Test, P_2 percent of the failures to X_2 UUT's and so on, with a fault isolation method
  - (2) Isolation of a specified percent of the failures to a specified quantity of LRU and SRU's at the various maintenance levels (on-aircraft, off-aircraft, base, depot)

- Fault isolation Resolution time:
  - (1) A specified percent of failures that occur within a specified maximum time
  - (2) A failure down to a replaceable level, within a specified average time
  - (3) A failure down to a replaceable level within a specified time once the failure isolation process has been initiated

- Mean-time-to-repair:
  - (1) System/equipment MTTR and maximum repair time
  - (2) System/equipment MTTR and maximum repair time at various maintenance levels

- BIT/ATE availability:
  - (1) Monitoring/fault isolation functions should be operating within a specified MTBF

- BIT/ATE mean time between failures:
  - (1) Mean time between failures of monitoring/fault isolation functions
  - (2) Mean time between failures of Automatic Test Equipment only

- BIT/ATE mean-time-to-repair:
  - (1) Mean-time-to-repair Automatic test Equipment
  - (2) Mean-time-to-repair monitoring/fault isolation functions

quantifiably measured and evaluated in terms of the initial system specification requirements and the emerging hardware configurations.

Table I-A-7-4 summarizes the effect of testability on the various design phase activities and the impact on the various integrity attributes. From this table, it can be seen that testability requirements are present in most of the design phase activities. If testability is taken into account and provided for in the design and development of the system, it can be assumed that, when deployed, the mean downtime (MDT) and mean maintenance time (MMT) will be minimized due to the availability of the proper test points and measures.

TABLE I-A-7-4. TESTABILITY INTEGRITY ATTRIBUTES

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.7. TESTABILITY	PRELIMINARY DESIGN PHASE: (1) Define Candidate System Architecture (5) Perform Maintainability Analysis (6) Establish Initial Man/Machine Task Allocation (7) Partition/Allocate Functions to Hardware/Software (8) Review Reliability/Maintainability Assessment Analysis (9) Prepare System Hardware Design/ Interface Specifications DETAILED DESIGN PHASE: (1) Review Specifications (2) Update Specifications and Drawings (4) Breadboard/Evaluate Circuits (5) Prepare Final Hardware Design Description	Maintainability Availability Reliability Testability Life Cycle Cost	MTTR MDT MMT	Time (Diagnostic/Repair) Cost (BIT/FIT/ATE Trade-off) % Faults Detected % False Alarms Fault Resolution Manpower/Training Costs Logistics Cost (Spares Provision) Maintenance Support Costs Test Equipment Complexity

APPENDIX I-A-8

I-A-8 Design Reviews (As a Measure of Integrity)

Design reviews are performed to evaluate reliability, maintainability, life cycle cost, performance, testing, and other characteristics of the emerging subsystem/system at specific design, manufacture and test points and milestones. The design review program should be established with both formal and informal reviews being identified that are consistent with the requirements of the procurement specification (statement of work) and the contractor's proposed program. The design review program should be structured to take into consideration:

- Review of all system elements down to the component level

- Review of all subcontractors design activities

- Identification of the participants and definition of their responsibilities

- Implementation of deficiency follow-up procedures

- Evaluation of performance with respect to milestones.

In order to be effective, the design review procedure should include a detailed/comprehensive checklist as well as criteria against which the design can be evaluated.

The design review participants should include system, design, component and reliability engineers as well as the appropriate management levels, and the informal reviews should include:

- Environmental Assessment Analysis

- Stress Analysis

- Reliability allocation/prediction

- Maintainability allocation/prediction

- Parts selection criteria

- Stress Screening plan/activities

- Design (circuit, packaging, board layout, etc.)

- Derating criteria

- Failure Modes Effects and Criticality Analysis

- Fault Tree Analysis (based on generic parts failures rates).

During the early design phase (preliminary design) the informal reviews should be conducted frequently in order to identify design changes (parts selection, derating, board layout, circuit design) at the lowest possible level. Design changes which are identified later in the design stage (detailed design) involve many drawings, parts lists, procurement and approval cycles, potential replacement of existing hardware and in effect are likely to be more costly. In addition, the informal reviews can facilitate detection and correction of actual or potential problems prior to finalization of design.

Formal Design Review

The formal design review program should consider:

- The overall system design

- The techniques and disciplines (resources) applied to the design effort

- Part selection criteria

- Derating

- Board design/layout

- Failure rates (predicted, analytically derived, measured)

- Thermal stress analysis and results

- Environmental stress analysis and results

- Subsystem/system integration

- Interface definition.

The design review should be controlled by an established agenda and should be based on detailed checklists (see Figure I-A-8-1), established internal procedures and standardized failure reporting, follow-up, and correction.

Preliminary Design Review (PDR)

The Preliminary Design Review (PDR) is performed after completion of the Preliminary Design Activities (when the initial "paper" design has been completed and documented). The PDR needs to be performed at the system, subsystem, module and part levels in order to insure that integrity as well as performance issues are being addressed. The PDR is used to determine that:

DESIGN REVIEW PROGRAM EVALUATION WORKSHEET/CHECKLIST

A. GENERAL INFORMATION

1) Program Specification: Title _____

Number _____ Program Manager _____

2) System/Equipment Description _____

3) Procurement Type _____ Criticality Level _____

4) Number of Units _____ 5) Contractor _____

6) Acquisition Phase: _____ 7) Contractor Documents _____

☐ Proposal _____

☐ Preliminary Design Phase   8) Submitted by _____

☐ Detailed Design Phase

☐ Prototype Development Phase

☐ Pre Production Phase

☐ Production Phase

9) Additional Information _____

B. R&M SPECIFICATION REQUIREMENTS

1) Design Requirements:

MTBF ($_o$) Subsystem A _____ hrs.   MTTR ($_o$) _____ hrs. _____

Subsystem B - _____ hrs.   Max Rp - _____ hrs.(95%) _____

Subsystem C - _____ hrs.

Subsystem D - _____ hrs.

composite: _____

2) Program Elements

	(R Level)		
	A	B	C
Reliability Program (MIL-STD-785) _____			
Parts Selection _____			
Derating _____			
Reliability Growth Testing _____			
Environmental Stress _____			
Failure Prediction _____			

FIGURE I-A-8-1.   Design Review Program Evaluation Worksheet/Checklist (Reference 2)

DESIGN REVIEW PROGRAM EVALUATION WORKSHEET/CHECKLIST — Pg 2

R&M SPECIFICATION REQUIREMENTS (Continued)

3) R&M Compliance

R Demonstration (MIL-STD-781)   Required å_____

M Demonstration (MIL-STD-471)   Required: _____

Acceptance (MIL-STD-781)   Required per Par: _____

4) Document Requirements	Req'd	Not Req'd	Comments
1. Reliability Program Plan	☐	☐	_____
2. Maintainability Program Plan	☐	☐	_____
3. Reliability and Maintainability Status Report	☐	☐	_____
4. Reliability Apportionment Report	☐	☐	_____
5. Reliability Prediction & Analysis Report	☐	☐	_____
6. Failure Mode Analysis Report	☐	☐	_____
7. Maintenance Concept Plan	☐	☐	_____
8. Maintainability Allocation Report	☐	☐	_____
9. Maintainability Prediction Report	☐	☐	_____
10. Part Selection, Control and Standardization Plan	☐	☐	_____
11. Deratin Guideline	☐	☐	_____
12. Critical Item Control List	☐	☐	_____
13. Subcontractor Reliability and Maintainability Control Plan	☐	☐	_____
14. Design Review Procedure & Checklist	☐	☐	_____
15. System Growth Test Plan/Procedure	☐	☐	_____
16. System Growth Test Report	☐	☐	_____
17. Reliability Demonstration Test Plan/Procedure	☐	☐	_____
18. Reliability Demonstration Test Report	☐	☐	_____
19. Maintainability Demonstration Test Plan/Procedure	☐	☐	_____
20. Maintainability Demonstration Test Report	☐	☐	_____
21. Failure Reporting and Corrective Action (FRACA) Procedures	☐	☐	_____
o Failure reports	☐	☐	_____
o Failure anlaysis reports	☐	☐	_____
o Corrective action reports	☐	☐	_____
o Failure summary reports	☐	☐	_____
22. Production Reliability Assurance Plan	☐	☐	_____
23. Reliability and Maintainability Assessment Reports	☐	☐	_____

FIGURE I-A-8-1. Design Review Program Evaluation Worksheet/Checklist
(Reference 2) (Continued)

- The design approach will meet the specification requirements in terms of performance and integrity.

- The design and proposed technologies are within the state-of-the-art (identification of risky approaches).

- The required design, manufacturing and test facilities are available.

- The proposed system can be designed, tested and built within the allocated resources of time, money and materials.

- The contractor, subcontractors, and vendors are technically qualified to produce the design parts and materials necessary to build the system.

Specific information and data to be reviewed at the PDR include:

- Design review plan

- Design review checklists

- Design review data packages

  - Part lists (standard, nonstandard, critical)
  - Circuit analyses (worst case, board layout, thermal analyses, etc.)
  - Reliability and maintainability allocations and predictions (based on generic part count/complexity)
  - Reliability plans (reliability growth, stress screens, etc.)
  - Trade-off study results (Reliability vs. cost, etc.)

- Problems (including potential solutions)

- Design changes.

At the successful completion of the PDR, the contractor can proceed with the detailed design.

Critical Design Review (CDR)

The Critical Design Review (CDR) is performed after completion of the detailed design, at a point where the final drawings are ready to be released to production to build the prototype subassemblies/system. This review provides the greatest potential for identification and correction of detailed design problem areas because it is conducted down to the part level at the time when the design is considered to be complete, all development and growth tests have been completed, and the output data from the PDR and the contractors informal reviews are available. The CDR will encompass much of

the same objectives and scope as the PDR; however, since this review repre-
sents the final opportunity to evaluate the design prior to reliability and
maintainability demonstration testing, it may prevent the start of costly
testing of a system that has not reached maturity.

A specific data package to support the conduct of the CDR should be
developed by the contractor in conjunction with the user. Included as part of
this data package would be the completed design review checklist and approved
as part of the PDR. Examples of the types of data necessary to support the
CDR include:

(1) System reliability and maintainability

(2) Total parts list (identifying nonstandard parts, with appro-
priate justification) including sources of supply and delivery
schedules

(3) Part derating application data

(4) Part failure rate data and sources (MIL-HDBK-217C/D, company
proprietary data bases, statistical study results, etc.)

(5) Failure mode, effects and criticality analyses/system safety
analyses

(6) Fault tree analyses

(7) Reliability prediction/assessment analysis

(8) Circuit analysis (including fault insertion test results)

(9) Reliablity growth test results

(10) Reliability and maintainability demonstration test plans and
procedures

(11) Production screening (thermal, vibration, AC power, etc.) and
acceptance test plans and procedures

(12) Technical configuration data including detailed block diagrams,
schematics, detailed drawings, parts lists, sources of supply,
data bases, test data, logs and records, etc.)

(13) CAD/CAM utilization/results

(14) System Integration Plan.

The Design Reviews provide a measure of integrity in many ways. The
most important of these is cost control. The major output of the design
review process is the identification of problems or potential problems and the
development of a plan to correct design problems, defects, etc. at the lowest

possible level. Problems discovered and corrected early in the design process are the least costly to fix and have the greatest impact on the integrity of the final product. Thus, the design review process when properly used can control the quality of the design and can affect the overall cost of the product substantially.

Table I-A-8-1 summarizes the effect of design reviews on specific design phase activities and the impact on the various integrity attributes. From this table, it can be seen that the Preliminary Design Review (PDR) and the Critical Design Review (CDR) if conducted at the appropriate time and in a well-planned manner, can result in the identification of problems or potential problems at the lowest cost points in the development cycle; and can impact the overall quality of the product by the resolution of reliability related issues. The informal as well as the formal design reviews provide the necessary feedback which can result in controlled costs both in the development phase and the production/development phases by identifying high-risk issues at an early time.

TABLE I-A-8-1. Design Review Integrity Attributes

Tools/Activity	Design Activity Affected	Integrity Parameter	Integrity Criteria	Integrity Measure
2.1.2.8. DESIGN REVIEWS	PRELIMINARY DESIGN PHASE: Informal as required in Activities 1 through 8 (9) Prepare System Hardware Design/ Interface Specifications DETAILED DESIGN REVIEW: Informal as required in Activities 1 through 4 (5) Prepare Final Hardware Design Description	Reliability Maintainability Availability Life Cycle Cost Produceability Supportability Testability Quality Assurance	MTBF MTTR MTBR	Product Quality Cost (Development/Testing) % Problems Detected/ Corrected Maintenance Support Costs Manpower/Facilities Cost

APPENDIX I-A-9

References - Design Phase (2.1)

1. The Avionics Integrity Program (AVIP), Dickman, T. J. and Cheshire, L. F. (Major), Federal Acquisition Research Conference/Symposium, December, 1983.

2. Reliability and Maintainability Implementation Notebook, Federal Aviation Administration (Airway Facilities Service) Volume 4, 1981.

3. Reliability and Maintainability Planning Notebook, Federal Aviation Administration (Airway Facilities Service) Volume 3, 1981.

4. Reliability Parts Derating Guidelines, Boeing Aerospace Company, RADC-TR-82-177, June 1982.

5. Navy Power Supply Reliability Design and Manufacturing Guidelines, NAVMAT P4855-1, Department of the Navy, December 1982.

6. Burn-In, An Engineering Approach to the Design and Analysis of Burn-In Procedures, Jensen, F. and Petersen, N. E., John Wiley and Sons, 1982.

7. Environmental Stress Screening Guidelines, ESSEH, Sponsored by the Institute of Environmental Sciences, Mandel, G. E., Jr., Chairman, 1981.

8. Navy Manufacturing Screening Program, NAVMAT P-9492, Department of the Navy, May, 1979.

9. Draft of ESDE "Environmental Stress Screening", USAF, Rome Air Development Center, 3 May 1982.

10. Integrated Assurance Assessment of a Reconfigurable Digital Flight Control System, Ness, et al, DOT/FAA/CT-82/154, Federal Aviation Administration, April, 1983.

11. A Review and Application of Analytical Models in Fault Tolerant Avionics Validation; Hitt, E. F., and Eldredge, D., IEEE/AIAA 5th Digital Avionics Systems Conference, October 31 - November 3, 1983.

12. Digital Flight Control System Validation; Eldredge, D. et al; 1982 American Control Conference, June 1982.

13. TEGAS-5, Time Based Logic/Fault Simulation and Test Generation System, Comsat General Integrated Systems, Inc., Palo Alto, California, 1982.

14. RADC Testability Notebook, Byron, J., Deight, L., and Stratton, G.; RADC-TR-82-189, Hughes Aircraft Company, June 1982.

15. Testing for Equipment Reliability with AC Power Cycling; Peterson, J.; Evaluation Engineering, April 1983, pp 70-73.

16. Research Study of Radar Reliability and Its Impact on Life Cycle Costs for the APQ-113, -114, -120, and -144 Radar Systems, General Electric Company, Aerospace Electronic System Department, Utica, New York, 1972.

17. Failure Analysis - Aims, Approaches, Applications, Wood, R. A., Battelle Technical Inputs to Planning/Report No. 36, Battelle Memorial Institute, Columbus, Ohio, 1983.